软件配置手册

—— μHammer3550-24/3550D-24/3550-48/3550D-48

港湾网络有限公司
北京市海淀区西三环北路 21 号久凌大厦
邮编：100089
电话：010-88512088 88512099
传真：010-68473171
E-mail：customer@harbournetworks.com
http://www.harbournetworks.com

P-(20)031103-130

版权声明

免责声明

本手册依据现有信息制作，其内容如有更改，恕不另行通知。港湾网络有限公司在编写该手册的时候已尽最大努力保证其内容准确可靠，但港湾网络有限公司不对本手册中的遗漏、不准确、或错误导致的损失和损害承担责任。

Users' Manual Copyright and Disclaimer

Copyright

Disclaimer

This document and the information contained herein is provided on an "AS IS" basis. Harbour Networks Limited may make improvements or changes in this documentation, at any time and without notice and as it sees fit. The information in this documentation was prepared by Harbour Networks Limited with reasonable care and is believed to be accurate. However, Harbour Networks Limited shall not assume responsibility for losses or damages resulting from any omissions, inaccuracies, or errors contained herein.

前言

本前言说明了此文档的大致内容、组织方式、针对用户类型、图标含义和其它文档。μHammer3550D-24 的软件配置与μHammer3550-24 相同，如无特殊说明，本手册只提及μHammer3550-24。μHammer3550D -48 的软件配置与μHammer3550-48 相同，如无特殊说明，本手册也只提及μHammer3550-48。

文档内容

μHammer3550-24/μHammer3550-48 上运行的操作系统 HammerOS(简称 HOS)，是由港湾网络有限公司自主研制开发。本手册介绍了 HammerOS 的功能、特性以及在μHammer3550-24/μHammer3550-48 上的配置方法，并且对所用到的命令给予了详尽的解释。

组织方式

章	题目	内容描述
第 1 章	HammerOS 概述	简述 HammerOS 的特性，包括 VLAN、Load Sharing、STP 等技术在交换机上的应用
第 2 章	访问交换机	讲述 HammerOS 系统的命令格式、用户权限的设置以及管理交换机的途径等
第 3 章	配置交换机的端口	讲述了交换机端口的基本参数配置，并针对如何解决 Load Sharing 作了详尽的介绍
第 4 章	ARP 管理	介绍 ARP 的相关知识及在交换机上的配置方法
第 5 章	FDB 表	讲述了 FDB 地址表的相关知识，以及如何在交换机上配置静态 FDB 地址表
第 6 章	虚拟局域网 VLAN	详细介绍了 VLAN 的作用、分类，以及如何在交换机上完成对 VLAN 各项的配置
第 7 章	生成树协议	讲述了 STP 和 RSTP，以及如何在交换机上进行相关配置
第 8 章	IGMP Snooping	介绍网络组管理协议的配置和应用
第 9 章	QoS	讲述了 QoS 知识及相关配置，包括 Queue、Dot1p、ACL 等内容
第 10 章	日志管理	介绍日志管理功能及设置方法
第 11 章	网络管理服务 NMS	讲述了网络管理服务模块的意义及在交换机上的配置方法
第 12 章	ACL 配置	讲述了 ACL 的相关知识及在交换机上的配置方法
第 13 章	SNTP 协议	讲述了 SNTP 的特性及在交换机上的配置方法
第 14 章	虚拟堆叠	讲述了虚拟堆叠技术的特点及其在交换机上的配置方法
附　录	普通用户命令一览表 管理员命令一览表	普通用户和管理员的命令一览表

针对用户类型

本手册主要是针对有一定网络知识的用户，以及负责组建网络设备并熟悉交换机配置的系统管理员。这要求读者熟悉以下知识：

- 局域网（Local Area Networks）（LAN）
- 以太网概念（Ethernet Concepts)
- 以太网交换和桥概念（Ethernet Switching and Bridging Concepts）
- 网络协议概念（Internet Protocol Concepts）
- 服务质量（Quality Of Service）(QoS)
- 简单网络管理协议概念（Simple Network Management Protocol）（SNMP）

图标说明

图标	作用
⚠	提示用户在配置交换机的过程中需要特别注意的地方
☞	表示给用户提示的附加说明信息

相关文档

1.《µHammer3550-24/3550D-24/3550-48/3550D-48 软件配置手册》 (本手册)

2.《µHammer3550-24/3550D-24 硬件安装手册》

3. 《µHammer3550-48/3550D-48 硬件安装手册 》

4. 《H.link 用户配置手册》

5. 《NAS 接入服务用户手册》

目录

第1章 HammerOS 概述

HammerOS 是港湾网络公司为 Hammer 系列交换机设计的操作系统，它运行在 FlexHammer、μHammer 及 BigHammer 系列交换机上。本章主要介绍了 HammerOS 的特性，以及相关技术的解释。

1.1 特性概述

在μHammer3550-24/μHammer3550-48 中 HammerOS 有如下特性：

- 支持IEEE 802.1Q和IEEE 802.1p标准的Virtual Local Area Networks (VLAN)
- 支持IEEE802.1d标准的Spanning Tree Protocol（STP）和IEEE802.1w标准的RSTP
- 线速（Wire-speed）二层交换
- 支持多端口到一个端口的镜像
- 支持端口捆绑 （Load sharing）
- 支持服务质量（QoS）
- 支持日志管理（Syslog）
- 支持IGMP Snooping
- 支持SNTP（Simple Network Time Protocol）协议
- 支持访问列表和数据包过滤
- 支持802.1x认证
- 支持H.Link
- 支持ACL安全访问特性
- 支持NMS网络管理服务
- 支持虚拟堆叠
- 支持Console 命令行配置
- 支持Telnet 命令行配置
- 支持Simple Network Management Protocol (SNMP)

**H.Link 是港湾网络有限公司的专有通讯协议。**

1.2 虚拟局域网（VLAN）

HammerOS 的 VLAN 功能使您在构建自己的广播域时，不再受限于网络的物理连接。一个 VLAN 就是一群独立于具体网络拓扑的设备，它们在通讯时，不论如何连接，属于这一 VLAN 的所有设备都好像在一个真正的物理局域网上。VLAN 的具体作用体现在：

- 可以控制广播数据，限制其广播的范围。假设在VLAN“研发部”中的一个设备发出了一个广播报文，那么只有“研发部”这个VLAN中的设备才能收到该广播报文，其他部门将不会收到。
- 提供了额外的安全特性。跨VLAN的访问只有通过三层转发，不能直接访问。例如，VLAN“市场部”的设备只能通过路由协议同VLAN“研发部”进行通信。
- 简化了设备在网络中的移动和管理。

具体来讲，VLAN 技术是为了创建第三层逻辑广播域，VLAN 可在一个 Switch 上划分，也可以跨越多个 Switch 划分。VLAN 实现了一个物理网段交换机群之间逻辑 LAN 划分，即分成多个逻辑广播域，避免广播风暴的发生。

**有关 VLAN 的详细配置信息见本手册第 6 章。**

1.3 生成树协议（STP 和 RSTP）

µHammer3550 交换机支持 IEEE802.1d 标准的 STP 协议，它提供了网络的动态冗余切换机制，使您能在网络设计中部署备份线路，并且保证：在主线路正常工作时，备份线路是关闭的；当主线路出现故障时自动使能备份线路，切换数据流。

RSTP 协议是依据 IEEE802.1w 标准，对 STP 802.1d 协议进行改进后的协议，它提供了网络的动态冗余切换机制，并在 P2P（非共享）链路上，能够进行端口状态的快速切换。在网络设计中可以使用 RSTP 协议来部署备份线路，保证在主线路正常工作时，备份线路关闭；在主线路出现故障时，自动快速启用备份线路，切换数据流。

**有关生成树协议详细配置信息见本手册第 7 章。**

1.4 Load Sharing

Load Sharing 技术是一种将网络流量聚集在一组端口上的方法，它可以形成交换机之间的大容量通道或容错通道，通道之间可以实现流量均衡。

HammerOS 支持 Load Sharing 功能，通过创建 Load Sharing 来提升交换机之间的带宽。Load Sharing 把多个物理端口捆绑在一起当作一个逻辑端口来使用。其作用表现在以下两个方面：

1. 如果 Load Sharing 中的一个端口发生堵塞或故障，那么数据包会被重新分配到该 Load Sharing 中的其他端口进行传输。
2. 如果这个坏掉的端口重新恢复正常，那么数据包将重新分配到该 Load Sharing 中的所有端口进行传输。

**HammerOS 的 Load Sharing 功能与 Intel 和 Cisco 同类产品的 Port Group 功能兼容。有关 Load Sharing 的详细配置信息见本手册第 3 章内容。**

1.5 IGMP Snooping 网络组管理协议

IGMP（Internet Group Management Protocol ）网络组管理协议是 IP 协议组中的一部分，用来支持和管理主机与组播路由器之间的 IP 组播。组播允许进行资源发现，使网络负载减到最小，在网上实现数据的有效传输。

IGMP snooping 用于监听主机与路由器之间的 IGMP 报文，并对监听到的 IGMP 报文进行处理。IGMP Snooping 使交换机能够跟踪与之物理相连的网络上每个组的成员。它在主机和直接邻接的组播路由器间运行，管理组成员关系。

**有关 IGMP Snooping 的详细内容请参阅本手册第 8 章。**

1.6 服务质量 (QoS)

QoS 是指 IP 的服务质量，也就是 IP 数据流通过网络时的性能。其目的是向用户业务提供端到端的服务质量保证，QoS 还提供了更高效的带宽使用率。HammerOS 系列交换机目前已经实现了端口优先级调度，802.1p 的 VLAN tag 到优先级的映射，ToS 到优先级的映射等多项相关服务。

**有关 QoS 的详细信息请参见本手册第 9 章**

1.7 日志管理（Syslog）

日志管理主要用来记录整个系统的运行情况以及用户操作行为。完整的日志管理能够帮助管理员及时了解和监控系统的工作情况，并实时记录系统的异常信息。

**有关 syslog 方面的详细内容请参阅本手册第 10 章。**

1.8 网络管理服务（NMS）

从安全的角度出发，我们在原有的访问控制基础上增加了新的控制，通过检查来访者的 IP 确定来访者是否有访问权限。只有通过合法的 IP 访问才可以建立连接，连接之后进一步检查用户名和密

码，都通过以后才可以访问和配置交换机。

**有关 NMS 的详细配置信息见本手册第 11 章。**

1.9 简单网络时间协议（SNTP）

简单网络时间协议 SNTP（Simple Network Time Protocol）是网络时间协议(NTP) 的一个简化本，用于同步因特网上的设备时钟。它与 NTP 的功能相同，只是比 NTP 更加简单。SNTP 可以在单播模式(点对点)和广播模式(点对多点)下操作，采用客户端/服务器的运行方式。在网络设备中运行 SNTP 协议有利于设备的管理和维护。

**有关简单网络时间协议 SNTP 的详细内容请参阅本手册第 13 章。**

1.10 802.1x 认证服务

μHammer3550-24/μHammer3550-48 支持 802.1x 认证服务器。IEEE 802.1x 称为基于端口的访问控制协议（Port based network access control protocol），该协议在利用 IEEE 802 LAN 优势的基础上，提供了对连接到局域网的设备或用户进行认证和授权的一种手段。通过此方式的认证，能够在 LAN 这种多点访问环境中提供一种点对点识别用户的方式。

μHammer3550-24/μHammer3550-48 采用了不同实现方式，即在开启 802.1x 功能时并不对 DHCP、IGMP、ARP、H.Link 和 vstack 报文的二层帧进行过滤，因此那些没有通过认证的用户尽管不能实现正常通信，但仍能够获取 IP 地址，并可进行 ARP 学习、建立 IGMP Snooping 组以及实现 H.Link 设备登录和虚拟堆叠管理等。

**有关 NAS 协议的详细信息请参阅《接入服务用户手册》。另外由于μHammer3550-24/ μHammer3550-48 不支持流量统计、基于 802.1x 的动态 ACL 修改，也不支持基于 802.1x 的带宽限制和多域认证。以下给出μHammer3550-24/μHammer3550-48 交换机和《接入服务用户手册》在命令上的差异：**

接入服务用户手册	碘ammer 3550-24/碘ammer 3550-48
以下命令参数或者参数的表达形式有变化	
config dot1x quiet-period <0-32767>	config dot1x quiet-period <0-65535>
config dot1x re-authentication period <1-32767>	config dot1x re-authentication period <1-65535>
config dot1x server-timeout <1-32767>	config dot1x server-timeout <1-65535>
config dot1x supp-timeout <1-32767>	config dot1x supp-timeout <1-65535>

<table>
<tr><td>config dot1x tx-period <1-32767></td><td>config dot1x tx-period <1-65535></td></tr>
<tr><td>config dot1x pae force-logoff mac <usermac> {port <portno>}*1</td><td>config dot1x pae force-logoff mac <address> {port <portno>}*1</td></tr>
<tr><td>config isp-domain <domain> accounting config-server id <id> type [primary|multi |backup]</td><td>config isp-domain <domain> accounting config-server id <0-4> type [primary|multi |backup]</td></tr>
<tr><td>config isp-domain <domain> authentication [add-server|delete-server] id <id></td><td>config isp-domain <domain> authentication [add-server|delete-server] id <0-4></td></tr>
<tr><td>config isp-domain <domain> authentication config-server id <id> type primary</td><td>config isp-domain <domain> authentication config-server id <0-4> type primary</td></tr>
<tr><td colspan="2">以下命令在碘ammer3550-24/碘ammer3550-48 交换机上不支持</td></tr>
<tr><td>config dot1x uplink-port <portno></td><td>不支持</td></tr>
<tr><td>config dot1x access-limit route-engine [rate|acl|disable]</td><td>不支持</td></tr>
<tr><td>radius config-attribute access-bandwidth [uplink|downlink] Vendor-Specific <VendorType> {<VendorId>}*1</td><td>不支持</td></tr>
<tr><td>radius config-attribute access-bandwidth [uplink|downlink] default-value</td><td>不支持</td></tr>
<tr><td>radius config-attribute access-bandwidth [uplink|downlink] standard <1-255></td><td>不支持</td></tr>
<tr><td>radius config-attribute access-bandwidth unit [bps|kbps]</td><td>不支持</td></tr>
<tr><td>radius config-attribute filter-id Vendor-Specific <VendorType> {<VendorId>}*1</td><td>不支持</td></tr>
<tr><td>radius config-attribute filter-id default-value</td><td>不支持</td></tr>
<tr><td>radius config-attribute filter-id standard <1-255></td><td>不支持</td></tr>
<tr><td>show dot1x access-limit route-engine</td><td>不支持</td></tr>
<tr><td>show dot1x uplink-port</td><td>不支持</td></tr>
<tr><td>show dot1x vlan <vlanname> pae</td><td>不支持</td></tr>
<tr><td>show dot1x vlan <vlanname> user-count</td><td>不支持</td></tr>
<tr><td>show radius config-attribute bandwidth-unit</td><td>不支持</td></tr>
<tr><td colspan="2">以下命令为碘ammer3550-24/碘ammer3550-48 特有的，没有写到《NAS 接入服务用户手册》中。</td></tr>
<tr><td>show isp-domain</td><td>显示系统中配置的所有域</td></tr>
<tr><td>show isp-domain <domain></td><td>显示域 domain 的详细配置信息</td></tr>
<tr><td>show radius config-attribute source-mac</td><td>显示使用哪个 RADIUS 属性携带用户的源 MAC 地址。</td></tr>
</table>

1.11 H.Link 远程集群管理

H.Link 协议是港湾网络有限公司的专有通讯协议，用以实现对远程设备的本地管理。用作 H.Link 服务器端的 μHammer3550-24/μHammer3550-48 可以同时管理多达 36 个互连的 μHammer1008/μHammer1016/μHammer1024 交换机，其工作原理是：服务器端使用 H.Link 协议，将多个远程客户端设备映射为本地虚拟子设备，通过虚拟子设备配置远程客户端设备，由此实现远程设备的本地化、集中化管理。此外，该协议还具有简单、可扩展、与平台无关等特点。

**有关 H.Link 协议的详细讲解请参阅港湾网络公司的《H.Link 用户配置手册》。**

第2章 访问交换机

本章主要介绍管理μHammer3550-24/μHammer3550-48 所需要的一些基本知识，包括：

- Bootromr启动
- 理解命令格式
- 常用命令
- 设置访问权限
- 管理交换机的途径
- 配置SNMP
- 配置静态路由
- 存取配置文件及升级HammerOS
- 网络状态及系统的检测

2.1 Bootrom 启动

Bootrom 启动分成两种方式：

- 自动启动
- 人工干预启动

2.1.1 自动启动

在默认方式下，交换机在上电之后，用户不需要干预，交换机将进入直接启动模式，启动信息显示如下：

```
Hammer Boot Loader version 1.1, Harbour Networks, Inc.
Compiled Fri 02-NOV-2001 11:00

Memory selftest: ................OK

Base ethernet MAC address: 00:05:3b:00:04:90

Copyright(c) 2000-2001 by Harbour Networks, Inc.
System booting...

Uncompress start...
Uncompress success, enter device initialize, Please wait...

Init console ... done.
Console baudrate is 9600.

Entering HammerOS ......
```

```
Initializing environment ...... Done.
Loading startup config ...... Done.

################################################################
#                                                              #
#                   Welcome to HammerOS.                       #
#                                                              #
#      Press Return to connect and config this system.         #
#                                                              #
################################################################
```

然后按回车键，进行用户登录。

2.1.2 人工干预启动

按照以下步骤可以访问 Bootrom 菜单：

1 连接交换机的 Console 端口，注意终端的正确配置。

2 打开交换机电源，并且不停的按空格键。

3 当出现“Hammer: ”提示符，说明已经进入 Bootrom 菜单。

人工干预启动后显示 Bootrom 菜单信息：

```
Hammer Boot Loader version 1.1, Harbour Networks, Inc.
Compiled Fri 02-NOV-2001 11:00

Memory selftest: ................OK

Base ethernet MAC address: 00:05:3b:00:04:90

Copyright(c) 2000-2001 by Harbour Networks, Inc.
System booting...

 ?         - List all available commands
 h         - List all available commands
 b         - Boot an executable image
 g        - Boot an executable image with default configurations
 u        - Load and boot an executable image
 l        - Load configuration file and boot an executable image
 r        - Reboot system

Press 'h' or '?' To get helping information.
Hammer:
```

Bootrom 菜单选项及其含义如下：

?：显示帮助信息

h：显示帮助信息

b：直接执行 HammerOS

g：使用缺省配置执行 HammerOS

u：使用 Xmodem 协议下载 HammerOS，并执行

l：使用 Xmodem 协议下载配置文件，并执行 HammerOS

r：重新启动交换机

2.2 理解命令格式

这一节主要讲述当您进入命令行进行配置时所要执行的步骤。请仔细阅读本节及后续内容中关于使用命令行接口的详细信息。使用命令行接口（CLI），请按照以下步骤：

第一步：当进入命令行接口出现命令提示符后，请确认您有相应的登录权限。

µHammer 3550 系列交换机的命令行系统支持两个不同的管理模式：一为只读模式，二为配置模式。在只读模式下只能对交换机的一般信息进行查看，没有配置权限。在配置模式下则有对交换机的配置权和所有信息的查看权。只读模式下的命令提示符是“Harbour>”，配置模式下的命令提示符是“Harbour(config)#”。

µHammer 3550 系列交换机的命令行系统对用户的划分也有两种：一为管理员用户，另一为普通用户。普通用户只能进入只读模式，管理员用户则可以进入任何模式，拥有所有的配置权限。

第二步：键入命令名称。

如果键入的命令不含需要用户输入的参数，那么请直接跳到第三步。如果键入命令中含有需要用户输入的参数，那么继续以下步骤：

1) 如果命令需要一个参数值，请输入一个参数值。在输入参数值时，可能要输入关键字。
2) 命令的参数值部分一般指定了您应该输入什么样的参数，是某范围内的数值，或者字符串或者 IP 地址。关键字是指命令中要操作的对象。
3) 如果命令需要多个参数值，请按命令的提示依次输入关键字和每个参数值。直到提示信息中出现<cr>按回车键信息为止。

第三步：输入完整的命令后，请按回车键。

例如：

用户不需要输入参数的情况：Harbour(config)#exit

“exit” 是一个不含参数和关键字的命令，当键入此命令后按回车则执行。

用户需要输入参数的情况：Harbour(config)#config port 2,3 speed 10

这是一个含有参数和关键字的命令。关键字为 port 和 speed，参数值为 2，3 和 10。

2.2.1 语法帮助

命令行接口中内置有语法帮助。如果您对某个命令的语法不太确定，请输入该命令中您所知道的前面部分，接着键入“?”或“空格＋？”。如果输入“?”则解释该命令；如果输入“空格＋？”则列出可以输入的关键字。命令行会提示您剩余部分可能的命令的清单。您就可以根据提示的命令继续输入，直至出现以下提示命令为止：<cr> Just Press Enter to Execute command! 这表明命令已输入完毕，按回车便可执行所键入的命令。

例如：

第一步：键入命令：who

第二步：如果接着输入“?”，系统显示如下信息：

who Display who is connected to the switch。

此信息说明 who 命令所要完成的功能；如果接着输入“空格+？”，系统显示如下信息：

am Display me myself who is connected to the target machine。

<cr> Just Press Enter to Execute command!

此信息说明 who 后面可以继续键入 am 构成新的命令，或者直接按回车键执行 who 命令。

2.2.2 使用语法帮助补齐命令

用户输入“Tab”键后，HammerOS 提供对命令进行补齐的功能。当您输入了一部分命令后，然后输入“Tab”键，如果匹配的命令有多个，则列出可能的命令清单，如果匹配的命令只有一个，那么命令行会自动把用户要输入的命令补齐，并把光标移至最后。

例如：

第一步：键入命令：ping

第二步：再输入一空格键，然后按“Tab”键，显示如下信息：

-t -count -size -waittime –ttl -pattern

以上信息就是命令 ping 之后可以继续输入的命令，然后按系统的提示信息继续键入您需要的命令。

如果一个命令比较长不好输入，您也可以使用“Tab”键。例如：

第一步：键入 show run

第二步：按“Tab”键，系统会自动补齐命令 show running-config

2.2.3 命令简写

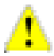
命令简写是指您可以只输入命令单词或关键字的前边部分字母，只要那部分字母不会造成歧义，交换机就能够识别该命令，用户可以直接回车执行该命令。但需要用户输入的参数，如 VLAN 的名

字(例子中为 market)等，要求完整输入。

例如：将端口 1-5 以 untagged 的方式加入到 market 虚拟局域网中，键入命令：

harbour(config)#config vlan market add port 1-5 untagged

上述命令也可简写为：con vl market ad po 1-5 un

 **当使用命令简写时，您必须输入足够多的字母，以确保在交换机的众多命令中不会造成歧义。**

2.2.4 命令中的符号

您可能会在命令格式中看到各种符号，这些符号只是说明您该如何输入该命令，但不是命令本身的一个部分。表 2-1 对这些符号进行了概要说明。

表 2-1 命令行中的符号

符号	描述
尖括号 < >	尖括号表示该命令的该部分必须输入一个参数。 例如命令：create vlan <name> 您必须在<name>那个位置输入一个合法的字符串作为您所创建的 vlan 的名字。
中括号 [ ]和竖直线 |	中括号一般和竖直线配合使用。中括号括起来的部分表示这部分命令有几个用竖直线分隔开的可选项，您必须选择输入其中一项。例如命令： config stpd default [enable|disable] 中括号内包含由竖直线分隔的两个可选项，您必须输入 enable 或者 disable。如果中括号中只有一个可选项，则直接输入那个可选项即可。
大括号 { }和星号 *	大括号一般和星号配合使用。大括号括起来的部分表示这部分命令可以不输入，也可以重复输入。重复输入的次数由大括号后紧跟的那个星号后的数字指定。 例如命令：show vlan {<name>}*1 表示您可以直接输入 show vlan ，也可以在 show vlan 后加上已经创建的某个 vlan 的名字。也就是说大括号中的命令可以输入 0-n 次。这个 n 的值由星号后的数字指定。

2.2.5 交换机的端口表示

对于µHammer3550-24/µHammer3550-48 来说，端口参数<portlist>可以有以下几种表示方法：

- 表示一个单独的端口：port 3　　表示端口 3
- 表示一个连续范围内的端口，中间用符号“-”连接：port 1-4　表示端口 1、2、3、4
- 表示多个端口，中间用逗号隔开：port　1-4，5，8　表示端口 1、2、3、4、5、8

2.2.6 命令参数类型

一般以尖括号“< >”括起来的部分是命令参数。HammerOS 的命令参数共有以下四种类型：

- 数值范围

  当尖括号中是两个由减号连接的数值时，表示该参数是取值范围在那两个数值之间的某个数。例如<1-255>表示用户可以输入大于等于 1 并且小于等于 255 之间的任意一个整数，比如 2 就是一个合法的数字。

- IP地址

  当尖括号中是 A.B.C.D 时，表示该参数是一个 IP 地址，您必须输入一个合法的 IP 地址值，例如 192.168.0.1 就是一个合法的 IP 地址值。

- 端口列表

  当尖括号中是 portlist 时，表示该参数是输入端口列表。端口列表中的多个端口之间用逗号“，”分隔，如果是连续的多个端口号可以用该连续端口的最小端口加上减号“-”再加上该连续端口的最大端口号表示。例如：输入 1，3-6，8 表示的端口列表为：1，3，4，5，6，8。

- 字符串

  当尖括号中所列的不是以上三种情况时，可能表示该参数需要输入的是一个字符串或者 16 进制数，具体可以在输入命令到该参数部分时，输入问号“？”键查看该部分参数的命令说明。例如：<macaddr> 表示要输入的是一个 16 进制的 MAC 地址，例如输入 005023344325 就是一个合法的 MAC 地址，而<name>则表示要输入一个字符串做为某个对象的名字。

2.2.7 行编辑命令

表 2-2 命令行中的行编辑命令

符号	描述
BackSpace 键或 Del 键或 Ctrl+h	向左删除一个字符
向上箭头键或 Ctrl+p	调用上一个历史命令
向左箭头键或 Ctrl+b	将光标向左移动一格
向右箭头键或 Ctrl+f	将光标向右移动一格
向下箭头键或 Ctrl+n	如果前边使用过向上箭头调用上一个历史命令，再单击向下箭头键可以显示下一个历史命

	令
Ctrl+a	将光标移动到行首
Ctrl+e	将光标移动到行尾
Ctrl+d	将光标所在位置的字符删除
Ctrl+k	将光标以后的字符全部删除
Ctrl+t	将光标所在的字符和光标左边的那个字符互相调换，并将光标向右移动一格
Ctrl+u	整行删除
Ctrl+w	将光标左边的字符全部删除

说明：上述命令中的 Del 键、向上箭头键、向左箭头键、向右箭头键和向下箭头键命令只支持利用 Telnet 配置交换机方式，不支持串口配置。而命令 Ctrl+h、Ctrl+p、Ctrl+b、Ctrl+f 和 Ctrl+n 对上述两种登录方式均支持。

2.2.8 命令模式

HammerOS 的命令行提供了两种模式，一种是只读模式，另一种是配置模式。在只读模式下用户只能查看一部分系统配置信息，在配置模式下用户能够查看所有系统配置信息，并能修改系统配置。

- 只读模式的提示符以“>” 结尾，表示为“Harbour>”，进入配置模式后，提示符以“#”结尾，表示为“Harbour(config)#”。只有管理员才能进入配置模式，并且要输入进入配置模式的密码。
- 在配置模式下输入命令“interface <vlanname>”，就会进入相应的接口配置模式，提示符为“HammerOS(config-if)#”。

有关只读模式和配置模式的详细信息请参阅本章后续内容

2.3 常用命令

2.3.1 enable

【命令作用】用于由只读模式进入配置模式

【命令格式】enable

【命令模式】只读模式

【使用指导】只读模式的提示符以“>”结尾，表示为“Harbour>”，进入配置模式后，提示符以 “#”结尾，表示为“Harbour(config)#”。只有管理员才能进入配置模式，并且要输入进入配置模式的密码。

【配置实例】由只读模式进入配置模式

```
Harbour>enable

Password：<enable-password>

Harbour(config)#
```

2.3.2 show history

【命令作用】HammerOS 能记住用户最近输入的 20 个历史命令。您可以使用以下命令 show history 来显示已经输入过的命令清单，同时您也可以用上下箭头键调用上一个或者下一个历史命令。详细内容可见上表：2-2。

【命令格式】show history

【命令模式】只读模式和配置模式

【配置实例】显示最近输入的历史命令

```
Harbour>show history

show history
list
show history
enable
show idle-timeout
exit
```

2.3.3 exit

【命令作用】退出当前模式，返回上一模式

【命令格式】exit

【命令模式】只读模式和配置模式

【使用指导】在只读模式下使用 exit 命令，将退出 HammerOS 系统，与 Quit，Logout 效果一样；在配置模式下使用 exit 命令将退回到只读模式。

【配置实例】在只读模式下使用 exit 命令

```
Harbour>exit

Exit
Disconnected.
Thanks for using Harbour Networks's product.
Bye!
```

在配置模式下使用 exit 命令

```
Harbour(config)#exit
Harbour>
```

2.3.4 show version

【命令作用】显示交换机的版本信息

【命令格式】show version

【使用指导】显示内容包括产品的硬件版本号、软件版本号、生产日期、产品序列号以及设备的 MAC 地址

【命令模式】只读模式和配置模式

【配置实例】在μHammer3550-24 交换机上显示版本信息

```
Harbour>show version

  Product    Name: μHammer3550-24
  Hardware Version: Version 1.22
  Bootrom  Version: Version 1.1
  Software Version: Version 1.2(Release 1.21  Apr 22 2003 10:17:33)
  Manufacture Date: 2002-12-26
  Serial   Number: 01010033A122022000001
  Base MAC Address: 00053b58013a

  Copyright(c) 2000-2001 by Harbour Networks, Ltd.
```

2.3.5 terminal length

【命令作用】设置终端每屏显示行数

【命令格式】terminal length <0-512>

【命令参数】length 指定的行数，范围从 0 至 512

【默认状态】每屏显示 20 行

【命令模式】只读模式和配置模式

【使用指导】如果参数 length 设为 0，则对每屏显示的行数不作限制

2.3.6 help

【命令作用】输出关于怎么使用“?”寻求帮助提示的文字

【命令格式】help

【命令模式】只读模式和配置模式

【配置实例】使用 help 命令

```
Harbour(config)#help

HammerOS provides help feature as described blow。
Anytime you need help, just press "?" and don't
press Enter you can see each possible command argument
and its description。

You can also input "list" and then press Enter
to execute this helpful command to view the list of
commands you can use。
```

该提示信息的大意是：通过以下两种方法，可以获得 HammerOS 提供的帮助信息：

一种方法是在命令行中输入“？”，不需按回车键，就可以看到每一个可能的命令参数以及相应的命令功能描述。

另一种方法是键入命令 list，按回车键，系统将显示当前命令模式下的所有命令清单，您可以从中选择需要的命令。

2.3.7 who

【命令作用】显示当前有哪些用户连接到目标机器

【命令格式】who

who am i

【命令模式】只读模式和配置模式

【使用指导】命令 who 显示所有连接到交换机的用户信息

命令 who am i 只显示自己（已与交换机连接）的信息

【配置实例】

```
Harbour(config)#who

SessionID - UserName ------- LOCATION ------- MODE ----
3             admin            console         CONFIG    (That's me。)
Total 1 sessions in current system

Harbour(config)#who am i

I am *Session [3] ： user admin connected from console。
```

2.3.8 list

【命令作用】显示当前模式下所有的命令

【命令格式】list

【命令模式】只读模式和配置模式

【配置实例】

```
Harbour>list

  clear
  enable
  exit
  help
  list
  logout
  ping  {[-t]}*1  {[-count]  <1-65535>}*1  {[-size]  <1-6400>}*1
   {[-waittime] <1-255>
}*1 {[-ttl] <1-255>}*1 {[-pattern] <user_pattern>}*1 <A.B.C.D>
  quit
  show ACL [<name>|all]
  show arp {[<A.B.C.D>|permanent]}*1
```



```
show fdb  {[mac] <macaddr>}*1 {[vlan] <name>}*1
show fdb agingtime
show fdb permanent {[mac] <macaddr>}*1 {[vlan] <name>}*1
show history
show idle-timeout
show interface {<IFNAME>}*1
show ip route
show ip route <A.B.C.D/M>
show ip route <A.B.C.D>
show ip route [connected|static]
（..............................省略了部分显示内容）
```

【相关命令】list<pattern>，该命令可根据关键字查找命令

2.3.9 show services

【命令作用】显示系统 services 状态

【命令格式】show services

【命令模式】只读模式和配置模式

【配置实例】

```
Harbour(config)#show services

Service telnet is up.
Service acl is down.
Service qos is down.
Service dhcprelay is down.
Service snmp agent is up.
Service snmp rmon is down.
Service snmp trap support is down.
```

2.3.10 quit/logout

【命令作用】关闭和目标机之间的连接，退出 HammerOS 系统

【命令格式】quit

logout

【命令模式】只读模式和配置模式

【使用指导】命令 quit 与命令 logout 作用相同

【配置实例】使用 quit 命令退出 HammerOS 系统

```
Harbour> quit

Quit.
Disconnected.
Thanks for using Harbour Networks's product.
Bye!
```

2.3.11 hostname

【命令作用】设置主机名称

【命令格式】hostname <hostname>

【命令模式】配置模式

【使用指导】在同一个网络中，最好统一规划主机名称

【配置实例】

```
Harbour(config)#hostname useA
useA(config)#
```

2.3.12 clear

【命令作用】清除屏幕显示

【命令格式】clear

【命令模式】任意模式

【使用指导】当屏幕显示内容太多，而且对您没有用处时，可以使用此命令

2.3.13 idle-timeout

【命令作用】设置系统的空闲超时时间。该时间是指对交换机进行的相邻两次操作之间所允许的最大空闲时间。当超过该时间时系统将自动执行 logout 操作。

【命令格式】idle-timeout <0-35791>

【命令模式】配置模式

【使用指导】<0-35791>表示空闲超时时间的范围，单位：分钟。当输入 0 时表示不对系统的空闲时间进行限制。

【配置实例】设置系统的空闲超时时间为 10 分钟

```
Harbour(config)#idle-timeout 10
```

【相关命令】show idle-timeout

该命令用于查看当前系统的空闲超时时间。

2.3.14 config timezone

【命令作用】配置交换机时区

【命令格式】config timezone <name> [positive|negative] <0-12> {<1-59>}*1

【参数说明】name 为本交换机时区名，输入 positive 表示在东区，输入 negative 表示在西区，<0-12>为小时数，<1-59>为分钟数。

【命令模式】配置模式

【配置实例】中国时区位于东 8 区

```
Harbour(config)#config timezone CST positive 8
```

2.3.15 show running-config

【命令作用】显示当前系统配置

【命令格式】show running-config

【命令模式】配置模式

【使用指导】这是一个很常用的命令，可以帮助系统管理员查看当前的系统配置情况

【配置实例】

```
Harbour(config)#show running-config
!HammerOS system config file ------------------------
!Syslog config
!Port config
!VLAN config
!FDB entry config
!Acl config
!Qos config
!Dscp config
!Tos config
!Bandwidth config
!Traceroute config
!Stpd config
!Route-policy rules config
!Interface config
!Static routes config
!Igmp snooping
!Arp config
!Sntp config
!Timezone config
!Dot1x config
!Port bind config
!RADIUS client config
!Usermanage config
!snmp config
!H.Link config
!Network access-control service config
!vstack cluster config
!end of config ------------------------------------
```

2.3.16 show startup-config

【命令作用】显示启动配置信息

【命令格式】show startup-config

【命令模式】配置模式

【使用指导】只有保存过系统配置文件才可以查看其内容

2.3.17 save configuration

【命令作用】保存当前的配置

【命令格式】save configuration

【命令模式】配置模式

【使用指导】如果您想让当前配置在交换机断电或重新启动后依然有效，切记一定要使用此命令保存您的配置

【配置实例】

```
Harbour(config)#save configuration

Trying save configuration to flash, please wait ......
Preparing configuration data to save...Done

Starting write configuration data to flash...Done。

Configuration save to flash successfully
```

2.3.18 erase startup-config

【命令作用】删除交换机中保存的系统启动配置信息

【命令格式】erase startup-config

【命令模式】配置模式

【使用指导】如果您想重新配置交换机的启动配置信息，请使用此命令删除以前的配置

【配置实例】

```
Harbour(config)#erase startup-config

Are you sure want to erase startup-config? [Y/N]y
Trying erase all configuration from flash, please wait ......
  finished
Successfully erase all configuration info from flash
```

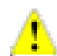
2.3.19 reboot

【命令作用】重新启动交换机

【命令格式】reboot

【命令模式】配置模式

【使用指导】重新启动交换机前，如果需要保存配置数据，请键入 save configuration。

 **如果您想使改变的配置在重新启动交换机或者交换机关机再开后仍然能有效，请切记在进行配置后使用"save configuration"命令把配置保存到交换机中。**

2.3.20 常用命令列表

表 2-3 命令行中只读模式下的常用命令

命令	描述

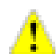
clear	清除屏幕显示
enable	进入配置模式，可以对交换机进行配置和写操作
exit	退出当前配置模式，返回到上一级配置模式
help	显示如何使用命令行中的语法帮助
list	显示当前可用的命令列表。
list <pattrn>	显示在当前模式下含有关键字 pattern 的所有的命令
logout	退出登录，断开连接
quit	退出命令行，断开连接（这个命令跟 logout 作用相同）
show history	显示已输入的历史命令
show services	显示当前系统提供的服务
show version	显示 HammerOS 的版本信息
who	显示当前连接到交换机的用户
show idle-timeout	显示 idle timeout（空闲超时）时间

只读模式下除了 enable 以外的所有命令在配置模式下都有效，所以在表 2-4 列出配置模式下常用命令时就不再重复这些命令。

表 2-4 命令行中配置模式下的一些常用命令

命令	描述
clear timezone	取消交换机的时区配置，恢复缺省时区配置
config timezone <name> [positive|negative] <0-12> {<1-59>}*1	配置交换机时区
enable-password	修改进入配置模式的密码，必须大于或者等于 6 个字符
erase {startup-config}*1	删除交换机启动配置
hostname <hostname>	设置系统的网络名称，例如，在本手册中，网络名称为 HammerOS
idle-timeout <0-35791>	设置经过多长的空闲等待系统自动进入登录前的状态
kill session <1-24>	强制断开特定 telnet 连接
login-password	设置登录密码
reboot	重新启动交换机
save configuration	保存系统配置信息
show interface {<IFNAME>}*1	显示接口状态
show running-config	显示系统的运行配置
show time	显示系统时间信息
show version	显示系统版本信息
terminal length <0-512>	设置终端屏幕所显示的行数
user add <username> login-password <login_password>	添加登录密码为<login_password>的用户<username>到系统中 hello|dd|ls-request|ls-update|ls-ack|all
user delete <username>	从系统中删除用户<username>

user enable-password <username>	设置用户<username>的配置密码
user list	显示所有系统用户
user login-password <username>	设置系统用户<username>的登录密码
user role <username> ADMIN enable-password <enable_password>	把用户<username>转变为系统管理员，且密码为<enable_password>
user role <username> NORMAL	把用户<username>转变为普通用户
who am i	仅仅显示用户自己的连接信息
reboot	重新启动交换机

 **HammerOS 命令行的所有命令都是不区分大小写的。**

2.4 设置访问权限

HammerOS 中提供了两种用户权限：

- NORMAL普通用户

  普通用户能查看大部分系统信息，但不能查看系统中的用户信息和系统的配置信息（主要指系统中的配置文件内容以及系统全局配置信息）。普通用户登录到 HammerOS 系统后，只能进入只读模式而不能进入配置模式。

- ADMIN 管理员

  管理员能进入配置模式并对系统的所有参数进行查看和设置。系统管理员还能增加用户帐号，删除用户帐号，设置修改用户密码，以及进行系统全局信息配置等。

2.4.1 系统缺省用户帐号

系统缺省内置了一个管理员用户帐号，用户名是 admin，缺省密码是 harbour。缺省用户 admin 的帐号不能被删除，用户也不能被修改，只能修改他的密码。

2.4.2 增加用户帐号

可以按照以下步骤建立用户帐号：

1. 以用户名 admin 登录（或者用任何其他管理员的用户帐号登录）；
2. 输入只读密码，进入只读模式；
3. 在只读模式下，输入 enable 命令，输入配置模式密码，进入配置模式；

4. 在配置模式下，利用以下命令创建一个用户帐号：

【命令格式】user add <username> login-password <login_password>

【参数说明】<username>是用户的名称，<login_password>代表用户登录密码。

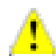
【使用指导】其中<username>是所要添加用户的名称，用户名必须为以字母开头的，只包含大写或小写的英文字母、数字、下划线且长度为 4-20 的字符串。<login_password>是该用户的登录密码，可以是由任意字符组成的长度为 6-20 的字符串。

【命令模式】配置模式

【配置实例】增加一个用户，用户名为 manager，登录密码为 harbour，在配置模式下，键入命令：

```
Harbour(config)#user add manager login-password harbour

Successfully added user manager as a NORMAL_USER ,
To change user role use “user role” command
```

 **系统对于用户名是不区分大小写的，对密码区分大小写。**

通过上述方法创建的用户一般都是普通用户，如果想要创建一个管理员的用户帐号，可以在按照以上步骤创建完用户帐号后，对用户权限进行修改。具体见本章下一节（修改用户权限）

2.4.3 修改用户权限

由于本系统中有两个不同级别的用户，所以通过以下两条命令可以将管理员用户转变为普通用户，也可以将普通用户转变为管理员用户。

将一个用户设为管理员，使用如下命令：

【命令格式】user role <username> admin enable-password <enable_password>

【参数说明】<username>是该用户的用户名，<enable_password>是该用户的登录密码。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#user add manager login-password 111111
Harbour(config)#user role manager admin enable-password 111222

Successfully change user manager to ADMIN mode.
```

将管理员设为普通用户，使用如下命令：

【命令格式】user role <username> normal

【参数说明】<username>是该管理员的用户名

【配置实例】将管理员用户 manager 的权限改为普通用户

```
Harbour(config)#user role manager normal

Successfully change user manager to NORMAL mode.
```


2.4.4 查看系统用户信息

查看用户列表，使用命令 user list

例如:在配置模式下，键入命令：user list。显示如下信息：

```
UserName --------- User_role ------
admin              ADMIN_USER
manager             NORMAL_USER
Total 2 users in system。
```

2.4.5 删除用户帐号

可以用以下命令删除一个用户帐号：

【命令格式】user delete <username>

【参数说明】username 是欲删除用户帐号的用户名。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#user delete manager

Successfully delete user manager .
```

2.4.6 修改密码

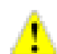
- 管理员修改自己的登录密码，在配置模式下输入 login-password。根据提示，输入新密码和确认新密码即可。
- 管理员除了能够修改自己的登录密码外，还能修改自己进入配置模式的密码，在配置模式下输入 enable-password。然后在提示符下输入新密码和确认新密码即可。
- 管理员还能够重新设置其他用户的密码，用以下命令：user login-password <username>、user enable-password <username>。并在提示符下输入新密码和确认新密码，就可以设置用户的登录密码和配置模式密码。

例如：修改用户 manager 的登录密码为 network，键入命令： user login-password manager

按回车，执行该命令。并输入新密码：network 和确认新密码：network。

修改用户 manager 进入配置模式的密码为 enter_config，键入命令：user enable-password manager

按回车，执行该命令。输入新密码： enter_config 和确认新密码： enter_config

 **注意：执行该命令必须确保 manager 是 admin 用户，否则系统会报错！**

2.5 管理交换机的途径

本交换机主要有以下几个管理途径：

- 使用一个终端（或者仿终端软件）连接到交换机的串口（Console），从而通过终端来访问交换机的命令行接口（CLI）。
- 使用Telnet管理交换机。
- 使用SNMP管理软件管理交换机。

本交换机同时能支持多个连接：

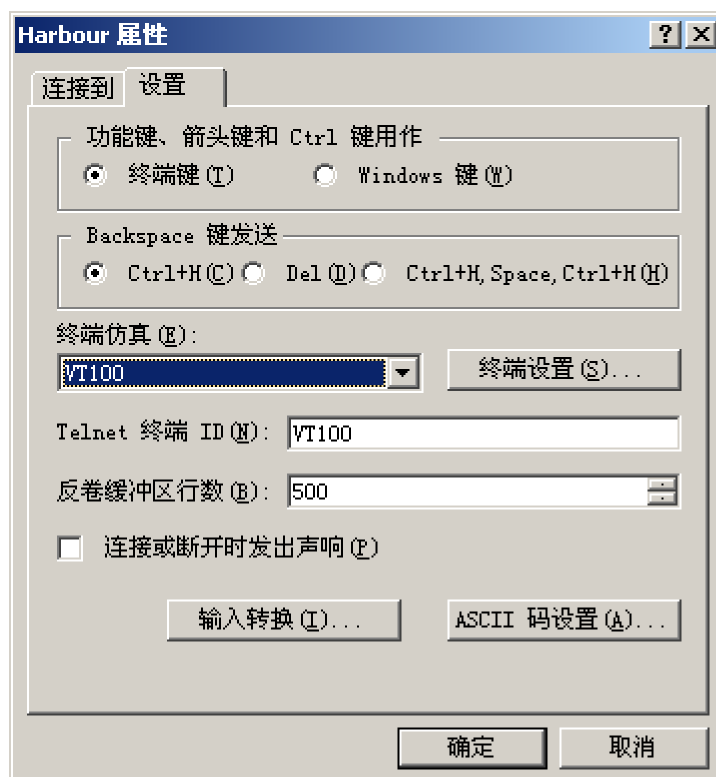
- 一个Console口连接
- 最多同时能支持3个telnet连接
- 最多同时能支持4个用户连接
- 一个用户最多同时开2个连接

2.5.1 使用 Console 口连接到交换机

可以通过在交换机前面板上标有“Console”字样的 RJ-45 串口与终端计算机的 COM 口相连。连接到 Console 端口的终端应按如下配置：

- 波特率： 9600
- 数据位： 8
- 奇偶校验：无
- 停止位： 1
- 流量控制：无

在使用 Console 口连接交换机时，推荐用户使用 VT100 终端仿真。设置方法：在超级终端界面中，打开“文件”菜单，选择“属性”工具条，出现一个窗口，点击“设置”标签，在终端仿真下拉列表中选择 VT100 即可。如下图所示：



如果连接成功，在终端中看到操作系统启动的界面后，您就可以通过命令行接口对交换机进行配置了。

例如：通过 Console 口连接登录到交换机后，我们给交换机配置一个 192.168.0.232 的 IP 地址，按以下步骤进行：

第一步：将交换机的 Console 口和特定终端连接起来，正常给交换机供电。

第二步：待 HammerOS 成功启动后，就可以看到交换机的提示登录信息：

```
############################################################
#                                                          #
#               Welcome to HammerOS。                     #
#                                                          #
#    Press Return to connect and config this system。      #
#                                                          #
############################################################
```

第三步：此时，系统要求您输入用户名和密码。

- 如果您是首次登录交换机，您就应该使用缺省的用户名 admin 进行登录，此时输入登录密码 harbour，按回车键，进入只读模式，输入 enable，按回车，键入配置模式缺省密码 harbour。
- 如果您已经分配了一个自己的用户名和密码，而且您已有系统管理员的权限，那么，登录时就使用自己的用户名和密码。

第四步：当您成功登录交换机时，系统显示如下信息：Harbour(config)#，表明您可以对命令行进行操作了。

第五步：然后给交换机的某个 VLAN（可以是 default VLAN 或者新创建的 VLAN，此处以 default VLAN 为例）配置 IP 地址。输入命令：config vlan default ipaddress 192.168.0.232/24。成功执行该命令后，就可以从该 VLAN 的端口上以该 VLAN 的 IP 地址 telnet 到交换机的命令行接口。

第六步：保存配置，键入命令：save configuration

```
Trying save configuration to flash, please wait ......
Preparing configuration data to save...Done。
Starting write configuration data to flash...Done。
Configuration save to flash successfully。
```

表明系统向 FLASH 中写入配置信息成功，即保存成功，而且所做的配置立即生效。

第七步：当您完成对交换机的操作后，键入命令：logout 或 exit 就可以断开与交换机的连接，并退出命令行界面。

2.5.2 使用 telnet 管理交换机

任何一个有 telnet 功能的工作站都能通过 TCP/IP 网络连接到交换机，从而实现对交换机的配置管理。如果使用 telnet 登录交换机，首先应该给交换机配置一个 IP 地址。然后在配置模式下输入命令：telnet <A.B.C.D>

 **注意：这里的参数<A.B.C.D>必须与本交换机的 IP 地址在同一网段。**

例如：远程登录一台 IP 地址为 192.168.0.232 的μHammer3550-24 交换机

在配置模式下，键入命令：

```
harbour(config)#telnet 192.168.0.232

Connected to 192.168.0.232。
Press Ctrl-Q to force exit telnet。
HammerOS Version1.1 on μHammer3550-48。
Login:
```

输入用户名和密码进行登录。

2.5.3 打开和关闭 Telnet 服务

以下命令可以打开或关闭 Telnet 服务，但您必须是以系统管理员的身份登录。

1. 打开 Telnet 服务：

【命令格式】service telnet enable

【配置实例】

```
Harbour(config)#service telnet enable

Successfully changed telnet service to up.
```

2．关闭 Telnet 服务：

【命令格式】`service telnet disable`

【配置实例】

```
Harbour(config)#service telnet disable

Successfully changed telnet service to down.
```

可以用 show service 命令查看系统提供的 Telnet 服务是否被打开：如果显示 Service telnet is up. 则表明 Telnet 已经打开；如果显示 Service telnet is down. 则表明 Telnet 已经关闭。

2.5.4 强制关闭一个非法 Telnet 连接

具有管理员权限的用户可以强制断开一个 Telnet 连接，步骤如下：

第一步：用 who 命令查看当前连接的用户。

第二步：如果发现有一个用户连接是非法的，那么可以根据用 who 命令所看到的该连接的 sessionID，然后用以下命令强制断开那个连接：kill session <1-24>，其中<1-24>是 sessionID 的取值范围。

如果您输入的 sessionID 是通过 console 口连接的，您将不能删除这个用户，此时系统会出现以下提示信息：You can't kill a console session.

通过强制关闭非法的 telnet 连接可以防止非法用户登录，从而提高系统的安全特性。

2.6 配置 SNMP

简单网络管理协议 SNMP（Simple Network Management Protocol）提供了一种监控和管理计算机网络系统的方法。当网络管理者利用 SNMP 管理交换机时，要求在管理平台上建立 Management Information Base（MIB 管理信息库），使网络中的所有变量都存放在 MIB 数据结构中。

2.6.1 打开或关闭 SNMP 服务

1．打开 SNMP 服务：

【命令格式】`service snmp enable`

【配置实例】

```
Harbour(config)#service snmp enable

Successfully changed snmp agent service to up.
```

2．关闭 SNMP 服务：

【命令格式】service snmp disable

【配置实例】

```
Harbour(config)#service snmp disable

Successfully changed snmp agent service to down.
```

可以用 show service 命令查看系统提供的 snmp 服务的状态：

如果显示 Service snmp agent is up，表明 snmp 服务已经被打开；

如果显示 Service snmp agent is down，表明 snmp 服务已经关闭。

2.6.2 SNMP 参数配置

对 SNMP 的参数配置使用以下命令：

【命令格式】config snmp community [readonly|readwrite] <string>

【使用指导】community 字符串为远程网络管理员配置交换机提供了一种用户确认机制。在交换机上有两种 Community 字符串：读确认 Community 字符串（readonly）允许对交换机进行只读访问，缺省值为 public。读写确认 Community 字符串（readwrite）提供了对交换机读写操作的权限，缺省值为 private。

【命令模式】配置模式

【相关命令】show snmp community-string

该命令可用于查看 SNMP 的 Community 字符串信息。

2.6.3 打开或关闭代理发送 trap 报文功能

【命令格式】service snmp trap [enable|disable]

【使用指导】选择 enable，表示打开代理发送 trap 报文功能；选择 disable，表示关闭代理发送 trap 报文功能。

【命令模式】配置模式

2.6.4 添加 trapreceiver

【命令格式】config snmp trapreceiver add <A.B.C.D> version [v1|v2c] {community <string>}*1

【使用指导】trapreceiver 是接收 trap 信息的主机；<A.B.C.D>为 traprceiver 的 IP 地址；v1/v2c 表示 trap 两个版本；如果这个 traprceiver 同时还承担对交换机的远程配置，那么可以为其设置 community 字符串。

【命令模式】配置模式

【配置实例】添加一个 trapreceiver，地址为 10.1.30.100，trap 的版本是 v1，键入命令：

```
Harbour(config)#config snmp trapreceiver add 10.1.30.100 version v1

Successfully added trapreceiver IP address is 10.1.30.100
The trap version is v1
The default trap community is public
```

2.6.5 删除 trapreceiver

【命令格式】config snmp trapreceiver delete <A.B.C.D>

【使用指导】<A.B.C.D>为 trapreceiver 的 IP 地址

【命令模式】配置模式

【配置实例】删除一个地址为 10.1.20.20 的 trapreceiver

```
Harbour(config)#config snmp trapreceiver delete 10.1.20.20
```

2.6.6 显示 trapreceiver 信息

【命令格式】show snmp trapreceiver

【命令模式】配置模式

【配置实例】显示 SNMP 的 trapreceiver 信息

```
Harbour(config)#show snmp trapreceiver

IP address            Version        Community
12.12.12.1             v1              public
Total 1 trapreceiver IP address in system.
```

2.7 配置静态路由

静态路由是由用户定义的一条可使数据包从源地址通过指定路径到达目的地址的路由。当动态路由协议未能创建一条到特定目的的路由时，静态路由就显得尤为重要。还可以通过配置某一静态路由为默认路由，把无路由的数据包发送到默认的网关。

2.7.1 增加静态路由

【命令格式】ip route <A.B.C.D/M> <A.B.C.D> {<1-255>}*1

ip route <A.B.C.D > <A.B.C.D> <A.B.C.D>{<1-255>}*1

【使用指导】第一个参数<A.B.C.D/M>为目的网段的 IP 地址和子网掩码长度，或者按照第二种命令格式将子网掩码由长度 M 的形式改为 IP 地址的形式。最后一个参数<A.B.C.D>为下一跳的 IP 地址。<1-255>表示路由的优先级，不设置时默认为 1，表示建立的这条静态路由具有最高优先级。

【命令模式】配置模式

【配置实例】添加一条去往 192.168.1.88 的静态路由，下一跳地址为 192.168.0.3。

```
Harbour(config)#ip route 192.168.1.88/24 192.168.0.3
```

或者可以用下一条命令增加一条静态路由信息：

```
Harbour(config)#ip route 192.168.1.88 255.255.255.0 192.168.0.3
```

2.7.2 删除静态路由

【命令格式】no ip route <A.B.C.D/M> <A.B.C.D> {<1-255>}*1

no ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> {<1-255>}*1

【使用指导】第一个参数<A.B.C.D/M>为目的网段的 IP 地址和子网掩码长度，或者按照第二种命令格式将子网掩码由长度 M 的形式改为 IP 地址的形式。最后一个参数<A.B.C.D>为下一跳的 IP 地址。

【命令模式】配置模式

【配置实例】删除一条去往 192.168.1.88 的静态路由，其下一跳地址为 192.168.0.3

```
Harbour(config)#no ip route 192.168.1.88/24 192.168.0.3
```

或者可以用下一条命令删除静态路由：

```
Harbour(config)#no ip route 192.168.1.88 255.255.255.0 192.168.0.3
```

2.7.3 显示静态路由信息：

【命令格式】show ip route

【使用指导】显示的内容包括目标 IP 地址、子网掩码和下一跳网关的 IP 地址。

【命令模式】只读模式和配置模式

【配置实例】

```
Harbour(config)#show ip route

***  begin route table info ***
Destination net-----NetMask----------Gateway-------
127.0.0.1       255.255.255.255      127.0.0.1
192.168.1.0      255.255.255.0       192.168.0.3
***  end route table info ***
```

2.7.4 配置静态路由命令列表

参数	描述
ip route <A.B.C.D/M> <A.B.C.D> {<1-255>}*1	添加一条静态路由，M 为子网掩码长度
ip route <A.B.C.D > <A.B.C.D> <A.B.C.D>{<1-255>}*1	添加一条静态路由，子网掩码采用 IP 地址的形式
no ip route <A.B.C.D/M> <A.B.C.D> {<1-255>}*1	删除一条静态路由，M 为子网掩码长度
no ip route <A.B.C.D> <A.B.C.D> <A.B.C.D>	删除一条静态路由，子网掩码采用 IP 地址的形式

{<1-255>}*1	
show ip route	显示静态路由信息
show ip route <A.B.C.D/M>	显示属于<A.B.C.D/M>网段的静态路由信息
show ip route <A.B.C.D>	显示目的地址为<A.B.C.D>的静态路由信息
show ip route [connected|static]	显示静态路由的 connected 信息或 static 信息
show ip route summary	显示静态路由的描述信息

2.8 存取配置文件及升级 HammerOS

在每次对交换机的配置进行修改后，都要对所做的修改进行保存。键入命令“save configuration”，将修改后的配置保存到交换机的扩展 FLASH 中。当显示如下字符串时：Configuration save to flash successfully。表明保存配置已经成功。

用户还可以把一份好的配置文件保存到文本文件中，在需要的时候（例如不小心把交换机配置搞乱了，不知道怎样把配置恢复到以前的状态时）再把配置文件下载到交换机中。下载可以有 2 种方法，可以用 FTP 下载，也可用 Xmodem 下载。

此外，用户可以将交换机中的配置文件内容上传到本地磁盘文件中，上传可以有 2 种方法，可以用 FTP 上传，也可用 Xmodem 上传。

2.8.1 通过 FTP 协议下载配置文件和 HammerOS

第一步：用具有管理员权限的用户通过串口或者 telnet 登录并进入配置模式。

第二步：输入命令 download ftp [config-file|hammeros] <A.B.C.D> <username> <password> <filename>。<A.B.C.D>为文件所在主机的 IP 地址，<username>是 FTP 的用户名，<password>为 FTP 用户的密码， <filename>为被下载的文件名。

第三步：等待下载完毕后，输入 reboot 命令重新启动交换机。

例如：假设地址 10.1.30.16 处存在一 FTP 服务器，并且此服务器上存在一个名为 sysconfig.txt 的配置文件，用户 useA 为此服务器的合法用户，密码是 harbour，在 HammerOS 配置模式下，输入命令：

```
Harbour(config)#download ftp config-file 10.1.30.16 useA harbour
  sysconfig.txt
```

系统显示如下信息

```
Trying download file from ftp server, please wait...

Successfully finished receiving file.

Trying write file to flash......
Finished.
```

```
You've successfully download new config file
Now you can type reboot command to reboot system.
```

2.8.2 通过使用 Xmodem 协议下载配置文件和 HammerOS

使用 Xmodem 协议下载文件，利用如下命令：

【命令格式】download xmodem [hammeros|config-file]{baudrate [9600|115200]}*1

【参数说明】选择 hammeros，下载文件为系统应用程序文件；选择 config-file，下载文件为系统配置信息文件，如果选择 baudrate 则用户可以选择下载文件的带宽：9600 或 115200

【配置实例】假设您机器上的 c:\windows\desktop 目录下存在一个系统配置文件：sysconfig.txt，把它下载到您的交换机上，可以如下操作：

第一步：用具有管理员权限的用户通过串口或者 Telnet 登录并进入配置模式；

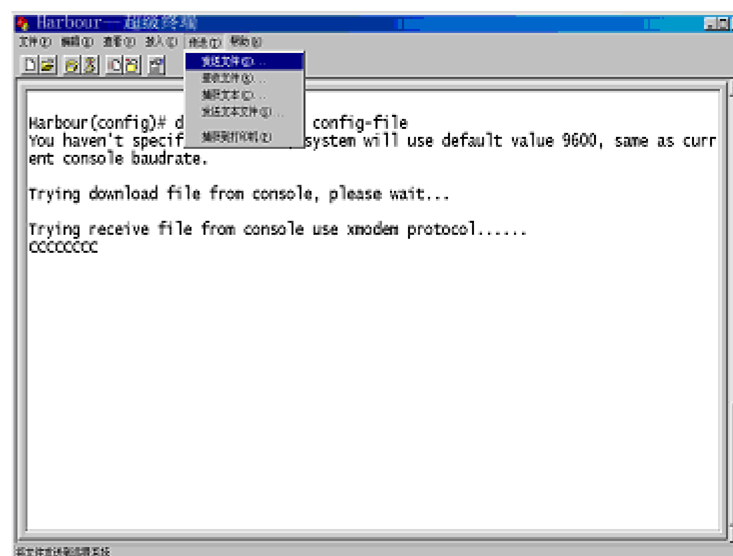
第二步：输入命令 download xmodem config-file。显示信息如下：

```
You haven't specified baudrate, system will use default value 9600, same as
    current console baudrate.

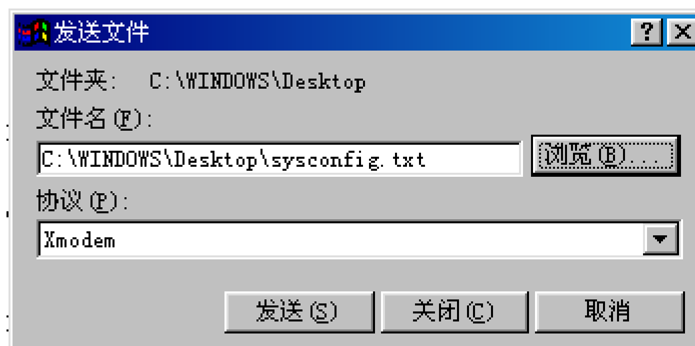
Trying download file from console, please wait...

Trying receive file from console use xmodem protocol......
CCC
```

第三步：打开串口超级终端的发送文件菜单



选择您所要下载的配置文件及协议（一定用 Xmodem）



选择“发送”，系统开始下载指定文件信息。



第四步：等待下载完毕后，显示下面信息，表明下载成功，

```
Successfully finished receiving file.

Trying write file to flash......Finished.

You've successfully download new config file
Now you can type reboot command to reboot system
```

输入 reboot 命令重新启动交换机。

```
Writing configuration to flash, please wait ...... finished.
Configuration saved to flash successfully.
```

2.8.3 通过 FTP 协议上传配置文件和 HammerOS

通过 FTP 协议上传文件，即将 Flash 中的文件上传到主机上，利用如下命令：

【命令格式】upload ftp [hammeros|config-file] <A.B.C.D> <username>
<password> <filename>

【参数说明】选择 hammeros，上传文件为系统应用程序文件；

选择 config-file，上传文件为系统配置信息文件。

<A.B.C.D>为 FTP 服务器的 IP 地址；

<username>为 FTP 服务器的用户名；

<password> FTP 服务器的密码；

<filename>为所生成的文件名。

【配置实例】假设地址 10.1.30.16 处存在一 FTP 服务器，并且此服务器上存在一个名为 sysconfig.txt 的空白文件，用户 useA 为此服务器的合法用户，密码是 harbour，并具有上传文件的写权限。在 HammerOS 配置模式下，输入命令：

```
Harbour(config)#upload ftp config-file 10.1.30.16 useA harbour
  sysconfig.txt
```

系统显示如下信息

```
Trying upload file to ftp server, please wait...
Successfully finished Upload file.
Finished.
You've successfully upload config file.
```

当前交换机的配置信息将被上传到 FTP 服务器指定目录下，以文件 sysconifg.txt 保存。

2.8.4 通过使用 Xmodem 协议上传配置文件和 HammerOS

通过 Xmodem 协议上传文件，即将 FLASH 中的文件上传到主机上，利用如下命令：

【命令格式】upload xmodem [hammeros|config-file]{baudrate [9600|115200]}*1

【参数说明】选择 hammeros，上传文件为系统应用程序文件；

选择 config-file，上传文件为系统配置信息文件。

如果选择 baudrate 则用户可以选择上传文件的带宽：9600 或 115200。不输入时，系统默认使用 9600。

【命令模式】配置模式

【配置实例】将系统应用程序文件上传到本地磁盘文件中，按以下步骤进行：

第一步：在配置模式下，键入命令：

```
Harbour(config)#upload xmodem hammeros baudrate 115200
```

按回车，显示如下信息：

```
System's current console baudrate is 9600.
You've choosen change console baudrate to 115200 when upload file.
Please change your terminal's baudrate to 115200 in 10 seconds.
After that, you can start receive file.
```

第二步：迅速改变终端的带宽为 115200bps

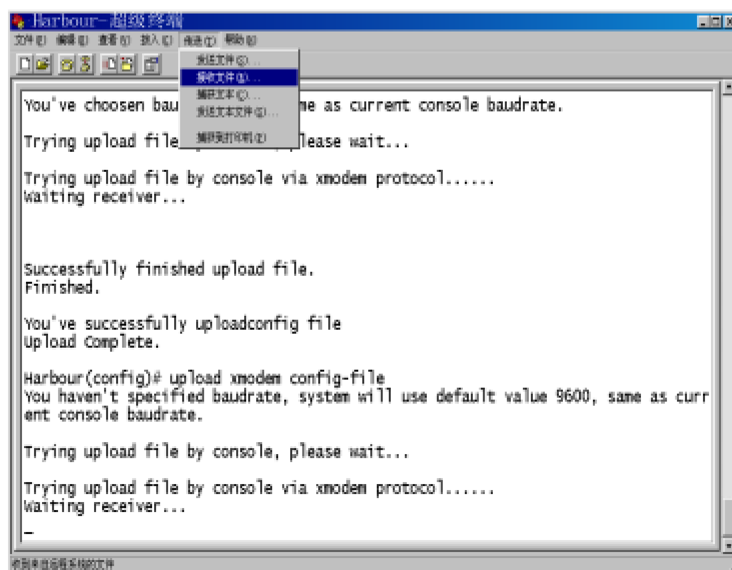
此时一定要在 10 秒之内改变终端的连接带宽为 115200bps，待完成操作后要恢复终端连接带宽为 9600bps 时，要先挂断再连并在 10 秒之内改回 9600。



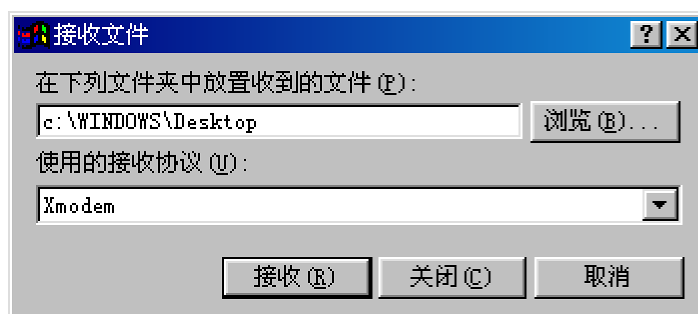
点击“配置”按钮后，在下图所示的端口设置中，将波特率设为 115200，然后点击“确定”即可。



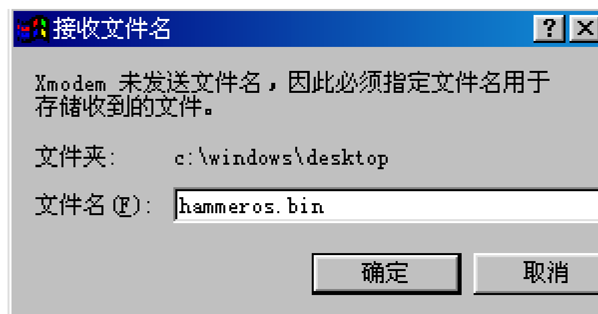
第三步：在超级终端中，选择传送菜单的“接收文件”



选择存放系统应用程序文件所在的目录，使用的接收协议是 Xmodem。



点击“接收”按钮，并输入系统应用程序文件名称，例如：hammeros.bin



点击“确定”按钮出现界面如下：



文件上传完毕出现如下提示信息：

```
Successfully finished upload file.
Finished.

You've successfully uploadimage file
Upload Complete.
```

到此为止，配置信息上传完毕。

 **通过文件的上传和下载，可以很方便地对多台相同配置的交换机进行配置。**

2.9 网络状态及系统的检测

2.9.1 用 ping 命令检测网络基本连接

交换机提供了 ping 命令用来检测网络的基本连接情况：ping 命令发送 Internet Control Message Protocol (ICMP) echo 消息到网络中的某个 IP 设备。普通用户和管理员用户都可以使用 ping 命令。ping 命令的语法是：

ping {[-t]}*1 {[-count] <1-65535>}*1 {[-size] <0-6400>}*1 {[-waittime] <1-255>}*1 {[-ttl] <1-255>}*1 {[-pattern] <user_pattern>}*1 <A.B.C.D>

ping 命令的众多选项可以都不输入，而使用最简单的格式。例如：ping 192.168.0.1，用来测试交换机是否可以跟 IP 地址为 192.168.0.1 的设备连接通信。如果设备连通，则出现以下信息：

```
PING 192.168.0.1 : 56 data bytes.
Press Ctrl-c to Stop.

Reply from 192.168.0.1 : bytes=56: icmp_seq=0 ttl=128 time=100 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=1 ttl=128 time=33 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=2 ttl=128 time=16 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=3 ttl=128 time=0 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=4 ttl=128 time=33 ms
```

```
----192.168.0.1 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss

round-trip(ms) min/avg/max = 0/36/100
```

如果设备没有连通，出现以下信息：

```
PING 192.168.0.1 : 56 data bytes.
Press Ctrl-c to Stop.

Request time out.
Request time out.
Request time out.
Request time out.
Request time out.

----192.168.0.1 PING Statistics----
5 packets transmitted, 0 packets received, 100% packet loss
```

表 2-5 ping 命令选项

参数	描述
-t	使用 t 选项后，ping 命令将一直向目标 IP 地址发送 ICMP echo 消息，直到用户用 Ctrl+c 中断。缺省不用 t 选项时，ping 命令发送完 5 个 ICMP echo 消息就停止发送了。
-count <1-65535>	count 选项指定 ping 程序总共发送多少个 ICMP echo 消息后就退出 ping 程序。
-size <1-6400>	size 选项指定发送的 ICMP echo 消息的附加内容长度。
-waittime <1-255>	waittime 选项指定 ping 程序等待多少秒之后如果还未收到应答就认为目标不可通。
-ttl <1-255>	ttl 选项指定 ICMP 数据包的 ttl（time to live）值。
-pattern <user_patter>	pattern 选项指定 ICMP 数据包中用户自己定义的 1-16 个 16 进制数。

2.9.2 用 traceroute 命令检测设备间的报文行径

交换机提供了 traceroute 命令用来检测交换机到目的地之间数据报行进的路径。traceroute 命令发送 Internet Control Message Protocol (ICMP) echo 消息或者 UDP 报文到网络中的某个 IP 设备。只有管理员用户可以使用 traceroute 命令。traceroute 命令的语法是：

traceroute {[-a] <A.B.C.D>}*1 {[-f] <1-30>}*1 {[-m] <2-255>}*1 {[-p] <1-65535>}*1 {[-q] <1-10>}*1 {[-w] <1-65535>}*1 <A.B.C.D>

traceroute 命令的众多选项可以都不输入而使用最简单的格式。例如：traceroute 202.96.13.137。通

过该命令可以测试交换机发出的数据报到达 IP 地址为 202.96.13.137 的设备所经过的路径。如果交换机不能与目的 IP 设备连接通信，通过 traceroute 命令可以获知数据报的传输在路径中哪一个地方出现问题。

如果设备连通，则出现以下信息：

```
traceroute 202.96.13.137

Type Control-C to abort.
Tracing the route to 202.96.13.137

 1   10.7.4.1          < 10 ms   < 10 ms   < 10 ms
 2   10.8.1.1            < 10 ms     16 ms     16 ms
 3   10.4.1.254            16 ms     16 ms   < 10 ms
 4   10.1.0.144            16 ms   < 10 ms     16 ms
 5   218.244.39.98          16 ms     16 ms     16 ms
 6   218.244.36.157         66 ms     50 ms     50 ms
 7   202.96.6.181          266 ms     66 ms     66 ms
 8   202.96.6.81           50 ms     66 ms     66 ms
 9   202.96.13.137          50 ms     66 ms     50 ms
```

如果设备没有连通，出现以下信息：

```
traceroute 202.96.13.137

Type Control-C to abort.
Tracing the route to 202.96.13.137

 1   10.7.4.1            < 10 ms  < 10 ms  < 10 ms
 2   10.6.1.1            < 10 ms    16 ms    16 ms
 3   10.4.1.254            16 ms    16 ms  < 10 ms
 4   10.1.0.144            16 ms  < 10 ms    16 ms
 5   218.244.39.98          16 ms    16 ms    16 ms
 6   218.244.36.157         66 ms    50 ms    50 ms
 7   * * *
 8   * * *
 9   * * *
```

输入 CTRL+C 可以中断 traceroute 命令，上述信息表明，交换机发出的数据报在 218.244.36.157 之前的路径上都能正常传输，但在 218.244.36.157 的下一跳出了问题。

交换机提供了两种 traceroute 的发包方式，用户可以选择发送 UDP 数据报或者 ICMP 数据报，UNIX 操作系统中的 traceroute 程序发送 UDP 报文，而 Windows 98 则发送 ICMP 报文。选择 traceroute 发包模式的命令格式为：config tracert_mode [udp|icmp]

表 2-6 traceroute 命令选项

符号	描述
-a <A.B.C.D>	设定 UDP 数据报源 IP 地址，该参数只对 udp 模式有效
-f <1-30>	指定数据报的初始 ttl（time to live）值，缺省值为 1
-m <2-255>	指定数据报的最大 ttl（time to live）值，即指定搜寻目的 IP

	设备的最大跳数，缺省值为 30
-q <1-10>	指定每一跳中的搜索次数，缺省值为 3
-w <1-65535>	指定 traceroute 程序每一次搜索所等待的时间，单位为秒，缺省值为 2

2.9.3 显示 CPU 利用率

使用以下命令显示 CPU 的利用率：show cpu usage。

例如：Harbour (config)#show cpu usage

```
cpu usage: 9%
```

2.9.4 显示内存状况

使用以下命令显示内存当前使用状况：show memory status

例如：Harbour (config)#show memory status

```
=================================================================
  =======
MODULE-NAME        32       64       128      256      512      1024
  2048
ROUTE          1104      6      1      5      0      0      2
VIRTUAL_END        0      0      0      0      1      0      0
MANAGE_CLI     24472   1375     73      2      6      0      0
RSTP             0      0      0      0    242      0      0
SLAB_SHOW         0      0      0      0      5      0      0
FDB              7      0      1     24      0      0      0
VLAN             0      0      1      0      0      0      0
ACL              0      0    240      0      0      0      0
RADIUS_CLIENT      3      1      1      0      0      0      0
ARP              0      1      0      0      0      0      0
TIMER             0      5      0      0      0      0      0
MANAGE_USER        3      2      0      0      0      0      0
20               1      0      0      0      0      0      0
QoS              4      0      0      0      0      0      0
IGMP_SNOOPING      2      0      0      0      0      0      0
=================================================================
  =======
MODULE-NAME       4096    8192    16K     32K     64K     128K
ROUTE            0      29      0      0      1      0
VIRTUAL_END        2      0      0      0      0      0
MANAGE_CLI        1      0      0      0      0      0
RSTP             0      0      0      0      0      0
SLAB_SHOW         0      0      0      0      0      0
FDB              0      0      0      0      0      0
VLAN             0      0      0      0      0      0
ACL              0      0      0      0      0      0
RADIUS_CLIENT      0      0      0      0      0      0
ARP              0      0      0      0      0      0
TIMER             0      0      0      0      0      0
MANAGE_USER        0      0      0      0      0      0
```



```
20               0      0     0      0      0      0
QoS              0      0     0      0      0      0
IGMP_SNOOPING      0      0     0      0      0      0
===========Total             CacheSize:1720320             Total
  UsageMemSize:1498196==========
```


第3章 配置交换机的端口

这一章主要讲述如何使用 HammerOS 来配置μHammer3550-24/μHammer3550-48 的端口，主要包括：

- 打开或关闭指定端口
- 打开或关闭指定端口的自适应功能
- 配置端口速率
- 配置端口的半双工或全双工模式
- 配置端口的流控
- 配置多端口负载均衡组（Load Sharing）
- 端口镜像（Port mirroring）

交换机的端口可以连接 10Base-T、100Base-T 或者 1000Base-T 网络，可以工作在半双工或全双工模式，要求用户根据实际情况对其进行配置：

- 缺省情况下，HammerOS 将交换机的所有端口设置为自适应模式，HammerOS 根据端口对端的性能自动调整端口的速率和双工模式。
- 用户也可以手工配置端口速率、双工模式和流控模式。流控功能与自协商是相对独立的，可以分别配置。

3.1 端口基本参数配置

3.1.1 使能或关闭指定的端口

对于启动后的交换机，在缺省情况下，端口都是使能的。当然，您可以根据实际需要对各个端口的状态进行配置。 利用以下命令使能或关闭一个或多个指定端口：

【命令格式】config port [<portlist>|all] [enable|disable]

【使用指导】参数<portlist>与 all 用于控制所要配置的端口，portlist 表示端口列表，允许一次配置多个端口；all 表明对所有端口进行操作。enable 与 disable 两个参数选择其一，如果键入 enable，则使能需要配置的端口；如果为 disable，则关闭这些端口。

【配置实例】关闭端口 1，3，5，7－12，配置如下：

```
Harbour(config)#config port 1,3,5,7-12 disable
```

3.1.2 配置端口的自适应模式

【命令格式】config port [<portlist>|all] auto [on|off]

【使用指导】参数<portlist>为端口列表，选择 all 表示对所有端口进行操作。选择 on 表示使能端口的自适应模式；选择 off 表示关闭端口的自适应模式。

【配置实例】关闭端口 24 的自适应模式

```
Harbour(config)#config port 24 auto off
```

3.1.3 配置端口的速率

【命令格式】config port [<portlist>|all] speed [10|100|1000]

【使用指导】参数<portlist>为端口列表，选择 all 表示对所有端口进行操作。选择 10 表示端口速度设置为 10M 模式，选择 100 表示端口速率设置为 100M 模式。选择 1000 表示端口速率设置为 1000M 模式。

【配置实例】将端口 25 的速率设置为 100Mbps

```
Harbour(config)#config port 25 speed 100
```

**注意：**

- **碘ammer 3550-24/碘ammer 3550-48 以太网电口的速率只能是 10/100M，不可以配置为 1000M。扩展模块中如果插入的是千兆光模块，则其端口速度也不可以配置；如果是千兆电口模块，可以配置相应端口速率为 1000M 模式，但必须指明端口的主从关系，参见下一节内容。**
- 只有关闭端口的自适应模式才可以进行端口速率的配置。

3.1.4 配置千兆电口的主从模式

【命令格式】config port [<portlist>|all] mode [master|slave]

【参数说明】参数<portlist>为端口列表，选择 all 表示对所有端口进行操作。
选择 master 把端口设置成主模式；选择 slave 表示把端口设置成从模式。

【使用指导】由于碘ammer 3550-24/碘ammer 3550-48 的上行端口可以是光口也可以是电口，如果是光口，其速率固定为 1000M，如果是电口，且您已手动指定了端口速率为 1000M，那么您还需要利用此命令将一端设置成主模式，另一端设置成从模式。

【命令模式】配置模式

3.1.5 配置端口的双工模式

【命令格式】config port [<portlist>|all] duplex [full|half]

【使用指导】参数<portlist>为端口列表，选择 all 表示对所有端口进行操作。选择 full 表示配置端口为全双工模式；选择 half 将端口设置为半双工模式。

【配置实例】将端口 24 设置为全双工模式

```
Harbour(config)#config port 24 duplex full
```

**注意：只有关闭端口的自适应模式才可以进行端口双工模式的配置。**

3.1.6 配置端口的流控

【命令格式】config port [<portlist>|all] flowcontrol [on|off]

【使用指导】参数<portlist>为端口列表，选择 all 表示对所有端口进行操作。选择 on 表示使能端口的流量控制功能；选择 off 表示关闭端口的流量控制功能。

【配置实例】使能所有端口的流量控制

```
Harbour(config)#config port all flowcontrol on
```

3.1.7 配置端口的地址学习功能

我们可以手工指定端口的地址学习功能：

【命令格式】config port [<portlist>|all] learn [on|off]

【参数说明】<portlist>表示端口的列表，all 表示所有的端口。选择 on 表示使能该端口的学习功能，选择 off 表示关闭该端口的学习功能。

【命令模式】配置模式

【配置实例】关闭端口 3 和 4 的自适应功能，并设置端口的速度为 10Mbps，双工模式为半双工，同时使能端口的地址学习功能，依次键入下面命令：

```
Harbour(config)#config port 3,4 auto off

Harbour(config)#config port 3,4 speed 10

Harbour(config)#config port 3,4 duplex half

Harbour(config)#config port 3,4 learn on

Harbour(config)#show port 3

----------------------------------------------------------------
  ------
              Port:3 's Configuration Information

Link State       : Up             Port State       : Enabled
Port Type        : 100BaseT        Speed           : 10
Autonegotiation  : Disabled        Duplex           : Half
Flowcontrol      : Disabled        Learn State      : Enabled

Port VLAN ID     : 2047
Port VLAN Name   : default
Port Summary     : normal
----------------------------------------------------------------
  ------
```


注意：千兆光口不支持半双工，不能工作在 10/100 兆模式。

3.1.8 端口配置命令列表

表 3-1 HammerOS 的端口配置命令表

命令	描述
config port [<portlist>|all] [enable|disable]	使能或关闭指定端口
config port [<portlist>|all] auto [on|off]	使能或关闭指定端口的自适应功能
config port [<portlist>|all] speed [10|100|1000]	配置端口的速度为 10 Mbps 或者 100Mbps 或者 1000Mbps
config port [<portlist>|all] duplex [full|half]	配置端口的双工模式为全双工或者半双工
config port [<portlist>|all] flowcontrol [on|off]	使能或关闭端口的流控制功能
config port [<portlist>|all] mode [master|slave]	配置千兆电口的主从模式
config port [<portlist>|all] learn [on|off]	使能或者关闭端口的地址学习功能
show port [<portlist>|all] {[configuration|stats]}*1	显示指定端口的信息 输入 configuration 选项时显示端口配置信息 输入 stats 选项时显示端口流量统计信息 缺省不输入任何选项时显示端口配置信息

3.2 多端口负载均衡组

HammerOS 能够通过创建多端口负载均衡组(Load Sharing)来提升交换机之间的带宽和增加冗余备份功能，Load Sharing 把多个物理端口捆绑在一起当作一个逻辑端口来使用。例如在 VLAN 中所看到的 Load Sharing 就是一个逻辑端口。如果 Load Sharing 中的一个端口发生堵塞或故障，那么数据包会被分配到该 Load Sharing 中的其他端口进行传输。如果这个坏掉的端口恢复正常，那么数据包将分配到该 Load Sharing 中的所有端口进行传输，从而提升交换机之间的带宽。当一台交换机的两个以上端口要同时向相邻的交换机发送数据时，创建 Load Sharing 非常有助于提高传输速度。同时，Load Sharing 对客户间的数据包的顺序提供了保障。

本公司的 Hammer 系列产品都支持 Load Sharing 功能，同时与 Intel 和 Cisco 同类产品的 Port Group 功能兼容。

注意：必须在相互连接的两台交换机上都设置 Load Sharing， 并且要对每对直接连接的两个做对应配置，否则会在网络中造成回路，导致交换机不能正常工作。

3.2.1 Load Sharing 规则

要设置 Load Sharing，必须创建 Load Sharing 的一组端口。Load Sharing 定义必须遵从以下规则：

- 用Load Sharing连接两个交换机时，要求Switch 1中Load Sharing的端口和Switch 2中Load Sharing的端口按端口号大小次序依次对应连接。例如，Switch 1的Load Sharing组中包括端口1、2、3、4，Switch 2的Load Sharing组中包括端口6、7、9、10，当两台交换机进行Load Sharing连接时，端口连接的对应关系为：1－6，2－7，3－9，4－10。
- 建议Load Sharing成员端口的速率保持一致，且必须处于全双工状态。
- µHammer3550-24/µHammer3550-48最多可以设置6个Load Sharing组，每个Load Sharing组最多包含8个端口。
- 1个Load Sharing组相当于一个端口，因此在配置时，不得更改从端口的参数。
- 配置的load Sharing组中所有成员的自学习功能必须保证一致，推荐load Sharing组的成员端口都处于自学习功能打开状态。
- 定义一个Load Sharing组时要选取其中的一个端口作为主端口，这个主端口在逻辑上代表这个Load Sharing组。
- 一个Load Sharing组中的所有端口必须属于同一VLAN，且端口的tag模式也要相同。
- 当端口工作于secure模式时，不能创建Load sharing。
- 当从端口up，而主端口down的情况下，load sharing会创建失败。
- Config port [<portlist>|all] [normal|secure] 中portlist不能包含Load sharing从端口号。
- Config port [<portlist>|all] secure [permit|deny]中portlist不能包含Load sharing从端口号。
- Config port [<portlist>|all] secure [add|delete] macgroup [<macfiltername>|all] 中portlist不能包含Load sharing从端口号。

另外，由于µHammer3550-48 交换机内部由两块芯片堆叠而成，其中芯片 1 包括端口 1-12、25-36、50，芯片 2 包括端口 13-24、37-48、49，µHammer3550-48 交换机不能跨芯片建立 Load Sharing 组。具体而言，要建立一个 Load Sharing 组，只能在端口 1-12、25-36、50 或端口 13-24、37-48、49 范围内建立。µHammer3550-24 交换机则不存在这个限制。

3.2.2 创建一个 Load Sharing 组

【命令格式】`create sharing <master_portno> grouping <portlist>`

【使用指导】`<master_portno>`表示所创建的 `Load Sharing` 组的主端口号，对于µHammer3550-48 交换机，此参数取值范围为`<1-50>`，而对于µHammer3550-24 交换机则为`<1-26>`。`<portlist>`表示与该 `Load Sharing` 相关的端口列表。

【命令模式】配置模式

3.2.3 删除一个 Load Sharing 组

【命令格式】delete sharing <master_portno>

【使用指导】<master_portno>表示要删除的 Load Sharing 组的主端口号。对于μHammer3550-48 交换机，此参数取值范围是<1-50>，而对于μHammer3550-24 交换机则为<1-26>。

【命令模式】配置模式

3.2.4 配置成员端口的转发模式

【命令格式】config sharing <master_portno> select-mode <rtag>

【参数说明】<master_portno>表示 Load Sharing 组的主端口号。对于μHammer3550-48 交换机，此参数取值范围是<1-50>，对于μHammer3550-24 交换机则为<1-26>。<rtag>为端口的转发模式，包括以下几种模式：

- smac: 基于源 MAC 地址负载均衡模式
- dmac: 基于目的 MAC 地址负载均衡模式
- sdmac: 基于源和目的 MAC 地址负载均衡模式
- slip: 基于源 IP 地址负载均衡模式
- dip: 基于目的 IP 地址负载均衡模式
- sdip: 基于源和目的 IP 地址负载均衡模式

【命令模式】配置模式

3.2.5 配置 Load Sharing 例子

以下的例子定义一个 Load Sharing 组，包含端口 10-14，并以端口 12 为逻辑上的主端口。其中，端口 12 在逻辑上代表物理端口 10、11、12、13、14。指明 shaing 成员端口的转发模式基于源和目的 MAC 地址。

```
Harbour(config)#create sharing 12 grouping 10-14
Harbour(config)#config sharing 12 select-mode sdmac
```

在实际组网中，主端口会随实际物理网络连接状态的变化而改变。创建了 Load Sharing 后，在配置 VLAN 或 STP 时将该 Load Sharing 作为一个逻辑端口使用，使用当前状态下该 Load Sharing 逻辑上的主端口（如上例中的端口 12 代表整个 Load Sharing 组中的所有端口）指定该 Load Sharing。进行 VLAN 配置时，对该主端口的操作等同于对该 Load Sharing 组中的所有端口操作，并且将不能再对 Load Sharing 中的其他非主端口的端口进行操作。这样，通过对端口 12 的配置来完成对 Load Sharing 中所有端口的配置。例如关闭 Load Sharing 组中的端口 10，11，12，13，14：

```
Harbour(config)#create sharing 12 grouping 10-14
Harbour(config)#config port 12 disable
```

3.2.6 显示 Load Sharing 配置

【命令格式】show sharing

【使用指导】显示当前系统中正在运行的 Load Sharing 组信息。包括主端口以及组中所含的端口列表。

【配置实例】

```
Harbour(config)#create sharing 1 grouping 1-3,5,7
Harbour(config)#config sharing 1 select-mode sdmac
Harbour(config)#show sharing

Sharing information:
Master Port: 1       Group Ports: 1   2   3   5   7
Forwarding Port Selecting Mode : Source mac and Destination mac address
```

3.3 端口镜像

端口镜像通过将一个或多个端口的数据复制到指定的端口上来实现网络流量分析和错误诊断。μHammer3550-48 交换机支持端口镜像功能，端口镜像功能基于如下规则：

- 每一个设备中，只能将一个端口作为镜像的目标端口。
- 可以将多个端口镜像到一个端口。
- 可以分别设置镜像端口的发包或者收包。

根据μHammer3550-48 交换机内部由两块芯片堆叠而成的硬件特点，其中芯片 1 包括端口 1-12、25-36、50，芯片 2 包括端口 13-24、37-48、49，由于 mirror 不能跨芯片建立，因此建立端口镜像时只能在端口 1-12、25-36、50 或端口 13-24、37-48、49 范围内建立。μHammer3550-24 交换机不存在这个限制。

3.3.1 配置镜像目标端口

镜像目标端口，指数据复制到的目标端口。交换机的任何一个端口都可以作为一个目标端口。一台μHammer3550-24 只能设置一个镜像目标端口，一台μHammer3550-48 可以配置两个镜像目标端口。被设置为镜像目标端口的端口不能再被设置成镜像源端口。指定镜像的目标端口，利用如下命令：

【命令格式】config mirroring <mirrornum> to <port>

【使用指导】<mirrornum>为镜像配置索引号，<port>为镜像目标端口

【命令模式】配置模式

3.3.2 配置镜像源端口组的发包和收包

μHammer3550-24/μHammer3550-48 支持多端口到一个端口的镜像，并可以分别设置镜像源端口的

发包和收包，利用如下命令：

【命令格式】config mirroring <mirrornum> [add|delete] port [<portlist>|all] [egress|ingress]

【参数说明】

- mirrornum　表示镜像组的索引号
- add　表示向镜像组添加源端口
- delete　表示从镜像组中删除源端口
- portlist　表示指定的参与镜像的源端口
- all　表示所有源端口参与镜像
- egress　表示镜像所有源端口的发送包
- ingress　表示镜像所有源端口的接收包

【命令模式】配置模式

【配置实例】

镜像端口 1-10 的发送包

```
Harbour(config)#config mirroring 1 add port 1-10 egress
```

镜像端口 1-10 的接收包

```
Harbour(config)#config mirroring 1 add port 1-10 ingress
```

3.3.3 取消端口镜像

【命令格式】config mirroring <mirrornum> disable

【参数说明】<mirrornum>表示镜像组索引号

【命令模式】配置模式

3.3.4 显示镜像信息

【命令格式】show mirroring

【命令模式】配置模式

【配置实例】配置镜像目标端口为 5，镜像源端口为 6-12 的发送包，镜像源端口 25-30 的接收包，并显示镜像信息，命令如下：

```
Harbour(config)#config mirrror 1 to 5
Harbour(config)#config mirroring 1 add port 6-12 egress
Harbour(config)#config mirroring 1 add port 25-30 ingress
Harbour(config)#show mirroring

Mirroring information:
The port which mirror to    : 5
The ports which egress traffic mirror from : 6 7 8 9 10 11 12
```

```
The ports which ingress traffic mirror from : 25 26 27 28 29 30
```

3.4 端口安全配置

端口安全可以对端口的访问使能进行控制，使得端口可以按要求被配置在某个范围内允许使用，从而达到端口安全的目的。μHammer3550-24/μHammer3550-48 支持端口安全功能，端口安全功能基于如下规则：

1. 每个端口既可以工作在安全模式又可以工作在非安全模式，可以在两种模式之间进行任意的切换。
2. 端口既可以允许所有的地址使用（此时工作在非安全模式，此模式也是端口的缺省模式），也可以允许部分或不允许部分地址进行使用。当然，如果需要的话也可配置为所有的地址都不能使用。
3. 对于用户配置的静态 FDB 地址，无论端口是在安全或非安全模式，这些静态的 FDB 地址在对应的端口上都可以进行访问。也就是说，只要用户配置了某个端口的静态 FDB，在该端口的地址就可以正常工作。
4. 端口安全不能使用在端口学习状态关闭的情况下。

3.4.1 实现机制

控制端口的访问是通过设置端口的学习位来实现的，即禁止端口的硬件地址学习能力，同时将需要进行源地址学习的包送往 CPU，由软件处理该地址学习与否，从而达到基于包的源 MAC 地址控制端口转发。如果该端口允许该 MAC 地址的包访问就由软件设置软/硬件二层转发表，反之则不设置。

3.4.2 创建地址组

【命令格式】create macgroup <name>

【命令作用】创建地址组，地址组用于将一些地址汇集到一起，然后可以将这些地址组与端口进行相连，从而可以进行端口的安全控制。地址组的名称只能由数字或字母组成，并且必须以字母开头，长度不能超过 30。系统共允许创建 256 个地址组。

【参数说明】<name>为地址组的名称

【命令模式】配置模式

【配置举例】

```
Harbour(config)#create macgroup mactest
```

3.4.3 删除地址组

【命令格式】delete macgroup [<name>|all]

【命令作用】删除已经配置的地址组

【参数说明】<name>为已经创建的地址组的名称。选择 all，表示对所有 macgroup 进行操作。

【命令模式】配置模式

【配置举例】删除已经创建的名称为 macgroup 地址组

```
Harbour(config)#delete macgroup mactest
```

3.4.4 向地址组中添加/删除地址

【命令格式】config macgroup <name> [add|delete] <mac>

【命令作用】向/从地址组中添加/删除地址。操作的地址不能是多播或广播地址，只能是单播地址。添加地址的数量没有限制，但一个地址组中不能有相同的地址存在。地址的输入格式为 12 个数字或字母的组合。

【参数说明】<name>为地址组的名称。选择 add 表示向地址组添加地址；选择 delete 表示从地址组中删除已添加的地址；<mac>是实际要添加的地址。

【命令模式】配置模式

【配置举例】

```
Harbour(config)#config macgroup mactest add 001122334455
Harbour(config)#config macgroup mactest delete 001122334455
```

3.4.5 配置端口工作在安全或者非安全模式

【命令格式】config port [<portlist>|all] [normal|secure]

【命令作用】配置端口工作在安全或非安全模式：端口工作在非安全模式时，我们已经进行与端口安全相关的配置将不起作用，只有端口工作在安全模式这些配置才起作用。可以通过下面的命令在端口的模式之间进行切换。默认的端口安全模式为 permit。

【参数说明】<portlist>为端口的列表，选择 all 表示对所有端口进行操作；选择 normal 表示将端口配置为非安全模式；选择 secure 表示将端口配置为安全模式。

【命令模式】配置模式

【配置举例】配置端口 1 工作在安全模式

```
Harbour(config)#config port 1 secure
```

3.4.6 配置端口在安全模式下的状态控制

【命令格式】config port [<portlist>|all] secure [permit|deny]

【使用指导】端口工作在安全模式时，可以有两种控制状态：permit/deny。

1、如果选择 permit，则所有与端口相连的地址组中的地址（后面会介绍如何将端口与地址组相连）在此端口上将可以进行访问。注意：如果此端口没有与任何的地址组相连，则此时此端口将禁止所有的地址进行访问（如果配置了静态的 FDB 除外）。

2、如果选择 deny，则所有与端口相连的地址组中的地址将被禁止在此端口上进行访问。注意：如果此端口没有与任何的地址组相连，则所有的地址在此端口上都可以进行访问。如果此端口当前为非安全模式，执行该命令会自动将端口设置为安全模式。

【参数说明】<portlist>为端口的列表，选择 all 表示对所有端口进行操作。选择 permit，将状

态设置为允许状态；选择 deny，将状态设置为拒绝状态。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config port 1 secure permit
```

3.4.7 将地址组与安全端口关联（或取消关联）

【命令格式】config port [<portlist>|all] secure [add|delete] macgroup [<macfiltername>|all]

【使用指导】将地址组与安全端口进行关联（或者取消关联）。

将地址组与安全端口进行关联就可以结合地址组中的地址和安全端口的状态进行安全的控制。注意：如果此端口当前为非安全模式，执行该命令会自动将端口设置为安全模式，如果端口已经是安全的则不会改变端口当前的 permit/deny 状态控制。端口与地址组之间是多对多的关系。也就是说，一个端口可以关联多个地址组，一个地址组也可以关联多个端口。

【参数说明】<portlist>为端口的列表。选择 all 表示对所有端口进行操作；选择 add 表示将地址组与端口相连；选择 delete 表示将地址组与端口断开连接；macfiltername 为地址组的名称，规则同上；选择 all 表示将所有的地址组与端口关联（或者断开关联）。

【配置实例】

```
Harbour(config)#config port 1 secure add macgroup mactest
```

3.4.8 显示地址组信息

【命令格式】show macgroup {<name>}

【命令作用】显示地址组的信息：包括地址组的名称、所有的地址、与其进行连接的所有的端口。

【参数说明】<name>为地址组的名称，规则同上面提到的一样。如果不输入地址组的名称将显示所有地址组的信息。

3.4.9 显示每个端口的信息

【命令格式】show perport [<portist>|all]

【使用指导】显示端口的信息。显示每个端口是安全/非安全模式，如果是安全模式显示与其相关联的所有的地址组的名称，是 permit 还是 deny 控制状态；此端口所属的地址组是否是安全的；地址组的地址学习的使能控制。

【参数说明】<portlist>为端口的列表，选择 all 表示对所有端口进行操作。

3.5 广播包抑制（Boradcast Limit）

广播包抑制功能可以有效地控制端口每秒收到的广播包数量，有效地防止广播攻击。

3.5.1 使能/关闭广播包抑制功能

【命令格式】config Broadcast_Limit [enable|disable]

【参数说明】enable 使能广播包抑制功能；disable 关闭广播包抑制功能

【命令模式】配置模式

3.5.2 配置端口的广播包接收数量上限

【命令格式】config Broadcast_Limit <1-262143>

【使用指导】配置每个端口每秒最多可接收的广播包数量，超过此值的广播包将被丢弃，默认值为 4096。

【命令模式】配置模式

3.5.3 查看广播包抑制配置信息

【命令格式】show Broadcast_Limit

【使用指导】显示当前广播包抑制功能的配置状态信息

【命令模式】配置模式

【配置实例】目前广播包抑制功能打开，每个端口每秒最多接收 10000 个广播包

```
Harbour(config)#show broadcast_limit

State             Value
_ _ _ _ _ _ _ _ _ _ _ _ _ __ _ _ _ _ _ _

enable            10000
```

3.6 下行环路检测（Loop Detect）

如果交换机端口的下游存在不支持 STP 协议的设备，且这些不支持 STP 协议的设备的链路存在环路，则会形成广播风暴，从而影响整个网络的正常运行。针对这一问题的解决方法是：对端口下游链路环路进行检测，如果检测到交换机端口的下游存在环路，则自动 disable 这个端口。配置下行环路检测的命令如下：

config loopdetect enable　　使能端口环路检测

config loopdetect disable　　关闭端口环路检测

如果端口下游存在环路，则最多 10 秒之后，使用命令 show port <portlist>查看该端口信息时，会发现该端口被 disable，并有 self-looped 的说明。

例如：端口 22 的下游存在环路，在使能端口环路检测功能之前使用 show port 22 命令查看到该端

口的 Port State 为 Enabled。使能端口环路检测功能之后在查看端口 22 的信息，可以看到该端口的 Port State 为 Disabled（self_looped）：

```
Harbour(config)#show port 22

-----------------------------------------------------------------
  -----------
              Port:22 's Configuration Information

Link State     : Up            Port State     : Enabled
Port Type      : 100BaseT       Speed          : 100
Autonegotiation : Enabled        Duplex         : Full
Flowcontrol    : Disabled       Learn State    : Enabled

Port VLAN ID    : 2047
Port VLAN Name  : default
Port Summary    : normal
-----------------------------------------------------------------
  -----------

Harbour(config)#config loopdetect enable

Harbour(config)#show port 22

-----------------------------------------------------------------
  -----------
              Port:22 's Configuration Information

Link State      : Up                 Port State      : Disabled
  (self_looped)
Port Type      : 100BaseT       Speed          : 100
Autonegotiation : Enabled        Duplex         : Full
Flowcontrol    : Disabled       Learn State    : Enabled

Port VLAN ID    : 2047
Port VLAN Name  : default
Port Summary    : normal
-----------------------------------------------------------------
  -----------
```

在人工检查并排除端口下游的环路后，要使得 port 22 恢复正常，请先 disable 端口 22，再 enable 端口 22。按顺序执行命令：

```
config port 22 disable

config port 22 enable
```

第4章 ARP 管理

地址转换协议 ARP（Address Resolution Protocol）提供了主机的 MAC 地址与 IP 地址的映射。交换机会自动学习这种映射并维护映射表。如果对某些特定的主机，您不希望交换机通过自学习的方式获得它们的地址映射，因为在一个庞大的网络中这种学习可能需要占用一定的时间，同时也有学习不到的危险，您也可以通过手工的方式为这些主机建立静态的地址映射表项。

4.1 添加 ARP 表项

添加一条静态 ARP 表项，可以利用如下命令：

【命令格式】config arp add <A.B.C.D> <mac_address>

【参数说明】<A.B.C.D>代码创建静态 ARP 的 IP 地址，<mac_address>代表 IP 地址对应的 MAC 地址

【命令模式】配置模式

【配置实例】添加一个静态 ARP 表项：

```
Harbour(config)#config arp add 10.5.1.32 00E02B123456
```

4.2 删除某个 ARP 表项

【命令格式】config arp delete <A.B.C.D>

【参数说明】<mac_address>为所要删除的设备的 MAC 地址

【命令模式】配置模式

【配置实例】删除一个已经存在的 ARP 表项：

```
Harbour(config)#config arp delete 00E02B123456
```

4.3 查看 ARP 表

【命令格式】show arp {[<A.B.C.D>|permanent]}*1

【参数说明】<A.B.C.D>代表 IP 地址，permanent 代表手工创建的静态 ARP 表

【使用指导】当不输入任何参数时显示系统中所有 arp 表项信息，包括动态与静态。

输入 IP 地址<A.B.C.D>可以查看指定 IP 地址对应的 ARP 表。

输入参数 permanent 时查看系统中所有手工创建的静态 ARP 表。

【命令模式】只读模式或者配置模式

【配置实例】

```
Harbour(config)#show arp

ARP  TABLE  LIST:

IP  ADDRESS          MAC  ADDRESS              TYPE          REFERENCE
  USE
```

```
---------------------------------------------------------------------
  ----------
11.1.0.1            00:50:fc:3c:13:d0      DYNAMIC              0
  1
---------------------------------------------------------------------
  ----------
TOTAL :1
```

**说明：ARP 表项的容量为 4000 条；动态 ARP 的老化时间为 20 分钟**

4.4 显示所有创建的静态 APR 表项

【命令格式】show arp user

【使用指导】此命令用于显示所有创建的静态 ARP 表项。该命令与命令 show arp permanent 的不同之处在于：show arp permanent 只显示状态为 up 的端口的静态 ARP 表项；show arp user 显示所有端口（up 或 down）的静态 ARP 表项。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#show arp user

Begin to show arp config table information
Physics Address     IP Address           Interface
00:11:22:33:44:55   1.1.1.3               default
Total 1 information
End to show arp table information
```

4.5 显示 ARP 表项数

【命令格式】show arp summary

【使用指导】此命令用于显示 ARP 表中的所有 ARP 表项数

【命令模式】配置模式

【配置实例】

```
Harbour(config)#show arp summary

ARP table information
Total 2 information
```

4.6 清除 ARP 表

【命令格式】clear arp

【使用指导】此命令用于清除 ARP 表，执行此命令后，ARP 表中的所有动态和静态表项均被清除

【命令模式】配置模式

第5章 FDB 表

本章讲述了 FDB（Forwarding Database）地址表的内容和相关知识，以及如何在 μHammer3550-24/μHammer3550-48 上配置静态 FDB 地址表。

5.1 FDB 地址表概述

交换机从它的所有端口接收 Media Access Control (MAC)地址信息，形成 MAC 地址表并维护它。当交换机收到一帧数据时，它将根据自己的 MAC 地址表来决定是将这帧数据进行过滤还是转发。此时，维护的这张 MAC 表就是 FDB 地址表。

5.1.1 FDB 地址表的内容

HammerOS 的 FDB 地址表数目由产品决定，μHammer3550-24/μHammer3550-48 可以存储最多 8k 条地址表项。每个 FDB 地址表项都包含以下内容：

- MAC地址
- 与MAC地址关联的端口号（Port）
- 与MAC地址关联的VLAN的名称(VLAN name)
- 该FDB地址表项的标志(Flags)

FDB 地址表项的标志的含义：

System ：系统（交换机）自动产生的第三层静态 FDB 地址表项。

Permenant ：该 FDB 地址表项是一个静态地址表项。

Dynamic ：该 FDB 地址表项是一个动态地址表项。

L3 ：该 FDB 地址表项是一个用于三层转发的地址表项。

如果收到数据帧的目的 MAC 地址不在 FDB 地址表中，那么该数据将被发送给除源端口外该数据包所属 VLAN 的其他所有端口。μHammer3550-24/μHammer3550-48 的每一个 FDB 地址表项由 MAC 地址和 VLANID 唯一标识。

5.1.2 FDB 地址表的地址表项类型

MAC 地址表共有三种地址表项：

动态地址表项——最开始的时候，交换机 FDB 地址表中的所有地址表项都是动态的。如果经过一段时间（老化时间 Agingtime）之后，设备没有数据传输，那么该地址表项就会被删除。这样能防止地址表项变得过于庞大，当确信某个设备从网络中去除后，就把该设备的地址表项删除掉。当交换机关机重启动或者 reset 时，所有的动态地址表项都将被删除。

固定地址表项——如果老化时间（Agingtime）被设为 0，那么该地址表项将存储在 MAC 地址表中而不会被动态删除，直到交换机关机或者重启。

永久地址表项——永久地址表项将一直保存在 MAC 地址表中，即使交换机关机或者重启。永久地址表项必须由系统管理员手工设定。一个永久地址表项可以是一个单播地址，也可以是一个组播地址（本系统暂时不支持组播地址）。所有由命令行输入的静态地址表项都将被存储为永久地址表项。μHammer3550-24/μHammer3550-48 交换机最多能支持 1K 个静态地址表项。永久地址表项一经建立，不会老化，但会随交换机的配置变化而变化。

以下事件的发生都会引起永久地址表项被删除：

- 删除一个与FDB静态表项关联的VLAN
- 修改一个与FDB静态表项关联的VLAN的tag值
- 从VLAN中删除与FDB静态表项关联的一个端口

以下事件的发生都不会引起永久地址表项的变化：

- 一个端口被关闭（disable）
- 一个端口被堵塞（block）
- 一个端口down掉（link down）

5.1.3 一个地址表项怎样被加入到 FDB 地址表中去

FDB 地址表中的地址表项可以通过以下两个途径被加入：

- 交换机自学习。交换机可以根据收到的数据包的源MAC地址、端口、VLANID，来自动更新FDB地址表。
- 可以通过命令行接口手工增加地址表项到FDB地址表中。

5.2 配置 FDB 地址表

配置 FDB 地址表可以使用如表 5-1 所列的命令。

表 5-1 HammerOS 的 MAC 地址表配置命令表

命令	描述
config fdb agingtime [0|<10-1000000>]	设置 FDB 地址表中的地址表项老化时间，缺省值为 80 秒，值 0 表示该地址表项永远不老化。
create fdbentry <mac_address> vlan <name> port <portlist> {priority <0-7>}*1	创建一个静态的永久地址表项。 <mac_address>：数据包的目的 MAC 地址； <name>： 数据包所属的 VLAN；

	<portlist>：数据包转发的目的端口号 {priority <0-7>}：优先级

5.2.1 配置 FDB 地址表实例

添加一个静态地址表项到 FDB 地址表中，可以利用如下命令：

【命令格式】create fdbentry <mac_address> vlan <name> port <portlist> {priority <0-7>}*1

【参数说明】<mac_address>是 MAC 地址，<name>是 vlan 的名称，<portlist>是端口号，priority 是优先级

【命令模式】配置模式

【配置实例】添加一个静态地址表项到 FDB 地址表中：

```
Harbour(config)#create fdbentry 00E02B123456 vlan market port 4
```

通过此命令，使这个静态永久地址表项具有以下属性：

- MAC 地址是 00:E0:2B:12:34:56
- VLAN 名字是 market
- 端口号是 4

配置 FDB 地址表的老化时间，利用如下命令：

【命令格式】config fdb agingtime [0|<10-1000000>]

【参数说明】[0|<10-1000000>]是老化时间，单位是秒。选择 0 表示地址表项永远不老化，缺省值是 80 秒。

【命令模式】配置模式

【配置实例】将 FDB 地址表的老化时间设为 40 秒：

```
Harbour(config)#config fdb agingtime  40
```

5.2.2 删除 FDB 表中的地址表项

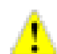
【命令格式】delete fdbentry {mac<mac_address> vlan <name>}*1

【参数说明】<mac_address>为所要删除的设备的 MAC 地址，<name>为所要删除的设备所属的 VLAN 名称。如果只是输入“delete fdbentry”，则删除所有的动态地址表项。

【命令模式】配置模式

【配置实例】删除 vlan market 中端口 4 的地址表项：

```
Harbour(config)#delete fdbentry mac 00E02B123456 vlan market
```

 **注意：对由系统创建的 FDB 表项不能删除。**

5.3 显示 FDB 地址表中的地址表项

5.3.1 显示 FDB 地址表中的所有地址表项：

【命令格式】show fdb {[mac]<macaddr>}*1 {[vlan]<name>}*1

【参数说明】<macaddr>代表 MAC 地址，<name>代表 VLAN 名

【使用指导】当 MAC 地址和 VLAN 名字一个都不输入时，将显示本交换机 FDB 地址表中的所有地址表项信息。当只输入 MAC 地址时，将显示本交换机所有 VLAN 中含该 MAC 地址的 FDB 地址表项。当只输入 VLAN 名字时，将显示此 VLAN 中的所有 FDB 地址表项信息。当既输入 MAC 地址又输入 VLAN 名字时，将显示该 VLAN 中此 MAC 地址的 FDB 地址表项信息。

【命令模式】只读模式或者配置模式

【配置实例】

```
Harbour(config)#show fdb

------- Begin of MAC Address Table Information (all)-------

MAC address       Port  vlan name                  Flags
------------------      ----      ------------------------------
  --------------------
00:05:3b:02:30:00   0    default                        System L3
  Permanent
00:05:3b:02:30:00   0     System Cluster                       System
  Permanent
00:05:4b:00:04:90   10   System Cluster              Dynamic
------------------      ----      ------------------------------
  --------------------
```

5.3.2 显示 FDB 地址表中的静态地址表项：

【命令格式】show fdb permanent {[mac] <macaddr>}*1 {[vlan] <name>}*1

【参数说明】<macaddr>代表 MAC 地址，<name>代表 VLAN 名

【使用指导】当 MAC 地址和 VLAN 名字一个都不输入时，将显示本交换机 FDB 地址表中的所有的静态永久地址表项信息。当只输入 MAC 地址时，将显示本交换机所有 VLAN 中含该 MAC 地址的静态地址表项。当只输入 VLAN 名字时，将显示此 VLAN 中的所有静态地址表项信息。当既输入 MAC 地址又输入 VLAN 名字时，将显示该 VLAN 中此 MAC 地址的静态地址表项的信息。

【命令模式】只读模式或者配置模式

【配置实例】

```
Harbour(config)#show fdb permanent mac 004532659872

-------      Begin      of      Permanent      MAC      Information
  (macaddr:[004532659872])-------

MAC address       Port  VLAN name            Flags
```

```
----------------- ---- -----------------------------
00:45:32:65:98:72   0    default              System
00:45:32:65:98:72   0    sun                 Permanent

----------------- ---- -----------------------------

Total 2 permanent mac showed.

----------  End of Permanent MAC Information ----------
```

5.3.3 显示 FDB 地址表的使用信息

【命令格式】show fdb usage

【使用指导】显示当前系统中 FDB 表的总数量以及动态和静态 FDB 表的数量信息。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#sh fdb usage

---------------- FDB usage ----------------
Static                         3
Dynamic                         0
Total                          3
-------------------------------------------
```

5.4 MAC 地址绑定

出于网络安全考虑，需要对接入用户进行控制，通过对交换机建立静态 FDB 实现 MAC 地址绑定，用以防止地址假冒。实现 MAC 地址绑定前，需要首先关闭交换机端口的地址学习功能，然后通过为该端口绑定一个静态 MAC 地址。这样，凡是来自该 MAC 地址的报文将允许通过，而来自其他陌生 MAC 地址的报文均被丢弃，从而限制了在该端口上允许通过的 MAC 地址。设置 MAC 地址绑定的步骤如下：

第一步：关闭端口的地址学习功能

config port [<portlist>|all] learn off

第二步：建立一条 FDB 地址表项以实现基于端口的 MAC 地址绑定

create fdbentry <mac_address> vlan <name> <portlist>

第6章 虚拟局域网 VLAN

6.1 VLAN 概述

简单地讲，VLAN 是指那些看起来好像在同一个物理局域网中能够相互通信的设备的集合。对于以端口划分的 VLAN 而言，任何一个端口的集合（甚至交换机上的所有端口）都可以被看作是一个VLAN。VLAN 的划分不受硬件设备物理连接的限制，用户可以通过命令灵活地划分端口，创建定义 VLAN。使用 VLAN 的优点如下：

1．VLAN 能帮助控制流量

在传统网络中，不管是否必要，大量广播数据被直接送往所有网络设备，从而导致网络堵塞。而 VLAN 的设置能够使每个 VLAN 只包含那些必须相互通信的设备，从而减少广播、提高网络效率。

2．VLAN 提供更高的安全性

每个 VLAN 中的设备只能与本 VLAN 中的设备通信。例如，如果 VLAN Market 的设备要和 VLAN Sales 的设备通信，则只有通过路由器才能进行，在没有三层路由设备的情况下两个部门不能直接通信，从而提高了网络安全性能。

3．VLAN 使网络设备的变更和移动更加方便

在传统网络中，网络管理员不得不在网络设备的变更和移动上花费大量的时间和精力。如果用户移动到另一个不同的子网，那么每个终端的地址都得重新设置。而使用 VLAN 则不需要这些复杂繁琐的设置。

6.2 VLAN 的分类

用户可以根据以下标准创建 VLAN：

- 物理端口
- 802.1Q tag
- 以上标准的组合

6.2.1 以端口划分的 VLAN

在一个 Port-Based VLAN（基于端口的 VLAN）中，用一个 VLAN 的名字来代表交换机中的一个或多个端口组成的一组端口。不同 VLAN 中的成员不能相互通信，即使它们在物理上属于同一个交换机的同一个 I/O 模块。如果要互相通信就必须通过三层交换机进行路由。这就意味着每一个 VLAN 的 IP 地址必须唯一，且不属于相同网段。

例如，在μHammer3550-48 交换机上，端口 1、9 和 15 属于 VLAN Market，端口 3 和 14 属于 VLAN Finance，端口 6、18-21 属于 VLAN Sales。

6.2.2 以标签划分的 VLAN

标签就是在以太网帧中插入的特定标记，称为 tag，它也是某个指定 VLAN 的标识号 VLANID。

 **使用 802.1Q 标签的数据包可能导致数据包长度比现行的 IEEE 802.3/以太网帧的最大字节数 1518 稍微大一点，这可能导致其他设备中的数据包计数错误，使得在含有非 802.1Q 网桥或路由器的网络中有可能导致连接出现问题。**

6.2.3 Tagged VLAN 的应用

标签（Tagging）最常应用在跨交换机创建 VLAN 的情况，此时交换机之间的连接通常称为中继。使用标签后，可以通过一个或多个中继创建跨多个交换机的 VLAN。一个 VLAN 可以很轻易地通过中继跨多个交换机。

使用 Tagged VLAN 的另一个好处就是一个端口可以属于多个 VLAN。这一点在某个设备（例如服务器）必须属于多个 VLAN 的时候特别有用，此设备必须有支持 802.1Q 的网络接口卡。

6.2.4 指定 VLAN 标签

每个 VLAN 都可被赋予一个 802.1Q VLAN tag。 当向一个由 802.1Q 标签定义的 VLAN 中添加端口时，您可以决定该端口是否使用这个 VLAN 的标签。HammerOS 交换机的缺省模式是所有端口都属于一个名叫 default 的 VLAN，其 VLANID 为 2047。

并不是所有端口都必须使用标签。当数据流从交换机的一个端口输出时，交换机实时决定是否需将该 VLAN 的标签加入到数据包中。交换机根据每个 VLAN 端口的配置情况决定加上或者去掉数据包中的标签。

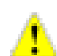
 **如果交换机收到带 tag 标记的数据包，当这个 tag 值与接收数据端口的 tag 值不同时，说明这个数据包来自其他 VLAN，因此交换机将丢弃该数据包。**

图 6-1 说明了使用 Tag（tagged）和未使用 Tag（untagged）划分 VLAN 的网络物理结构图。

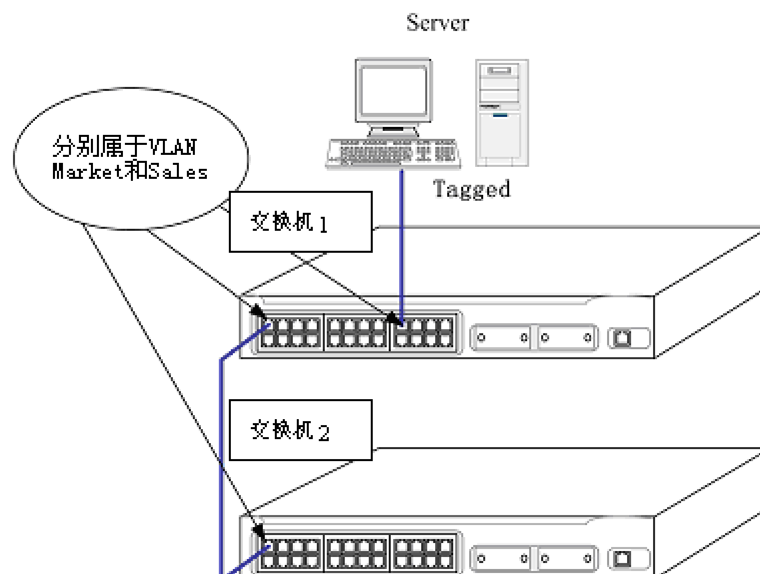


图 6-1 以 tagged 和 untagged 划分 VLAN

交换机 1 的端口 1 和交换机 2 的端口 1 同时属于 VLAN Market 和 VLAN Sales，且两个端口之间有中继线连接。跨交换机的 VLAN Market 和 VLAN Sales 通过这条中继线相连，从而实现跨交换机的 VLAN 通信。其中：

- 中继端口都为tagged。
- 连接到交换机1端口9上的Server须含有支持802.1Q Tagged的网络接口卡（NIC）。
- 连接Server的交换机1的端口9必须同时属于VLAN Market和VLAN Sales。
- 除了连接Server的交换机1的端口8和两台交换机的端口1是tagged以外，其他端口都是untagged。
- 当数据转发到交换机的端口时，交换机决定数据送达到目的端口是否需要加标签（tagged）。所有Server收发的数据都是加标签的（tagged）；从其余终端工作站收和发的数据都是untagged。

6.2.5 混合使用 Tagged VLAN 和 Port-Based VLAN

您可以混合使用 Tagged VLAN 和 Port-Based VLAN。一个给定的端口可以属于多个 VLAN，前提是该端口只能在一个 VLAN 中是未加标签的（Untagged)。换句话说，一个端口同时能属于一个 Port-Based VLAN 和多个 Tagged VLAN。

出于 VLAN 分类的目的，如果交换机收到一个含 802.1Q 标签的数据包，但是该 802.1Q 标签所含的 VLANID 的值为 0，那么交换机会把该数据包当作是未加标签的（untagged)。

6.3 配置 VLAN 的有关规则

Hammer 交换机的 VLAN 配置要求遵循一定的规则，我们对 VLAN 的命名、端口的添加、IP Address 的配置、Tag 值的范围等有一定的要求。

6.3.1 缺省 VLAN

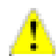
每一台 Hammer 交换机出厂时都有一个缺省的 VLAN，该 VLAN 有以下属性：

- VLAN 的名字是default
- 它包含所有端口
- default VLAN的所有端口都是untagged的
- default VLAN的VLANID是2047

6.3.2 VLAN 的名字

每个 VLAN 的名字可以是由以字母开头的 1 至 30 个字符组成，这些字符只能是字母、数字或者下划线 “_”。空格符、逗号、引号等字符都是不合法的。

VLAN 的名字只是本地标志。也就是说，在一台交换机上设置的 VLAN 的名字只对该交换机有意义。如果另一台交换机（Switch2）与该交换机(Switch1)相连，那么这个交换机(Switch1)的 VLAN 的名字对那台交换机（Switch2）来讲毫无意义。

 **您应该在整个网络中统一规划命名您的 VLAN。**

6.3.3 VLAN 端口的添加

µHammer3550-24/µHammer3550-48 的端口可以以两种形式属于某个 VLAN，分别是：IEEE 802.1Q tagged 模式 和 IEEE 802.1Q untagged 模式。一个端口在 IEEE 802.1Q untagged 模式下只能属于一个 VLAN，以 IEEE 802.1Q tagged 模式可以属于多个 VLAN。

添加 VLAN 端口，利用如下命令：

【命令格式】`config vlan <name> add  port <portlist> [tagged|untagged]`

【参数说明】<name>是 vlan 的名称，<portlist>是端口列表，选择 tagged 表示向 VLAN 添加 tagged 端口，选择 untagged 表示向 VLAN 添加 untagged 端口。

【使用指导】当我们向一个指定 VLAN 中添加 IEEE 802.1Q untagged 端口时：

如果该端口属于 Default VLAN，则该端口可以添加到指定的 VLAN 中，同时交换机会自动从 Default VLAN 中将该端口删除。

如果该端口不属于 Default VLAN，那么该端口肯定以 IEEE 802.1Q untagged 模式属于某个其他 VLAN，则不能将该端口添加到指定的 VLAN 当中。

当我们往一个指定 VLAN 中添加 IEEE 802.1Q tagged 端口时，不再受该端口与其他 VLAN 关系的限制。如果该端口已经以 IEEE 802.1Q untagged 模式属于该 VLAN 时，

端口可以添加成功，但该端口将不再以 untagged 模式属于该 VLAN。

【配置实例】创建一个名称为 market 的 VLAN，且端口 2 已经以 IEEE 802.1Q untagged 模式属于该 VLAN。

```
Harbour(config)#show vlan market

VLAN ID          : 2045
Name              : market
MAC address      : 00:45:32:65:98:72
Tagged Ports     :
Untagged Ports   : 2  4  5  8  9  10
```

当我们向 market 添加一个以 IEEE 802.1Q tagged 模式属于该 VLAN 的端口 2 时，键入命令：

```
Harbour(config)#config vlan market add port 2 tagged
Harbour(config)#show vlan market

VLAN ID        : 2045
Name           : market
MAC address     : 00:45:32:65:98:72
Tagged Ports    : 2
Untagged Ports  : 4  5  8  9  10
```

此时，端口 2 以 IEEE 802.1Q tagged 模式属于 market，所以 untagged ports 中就没有端口 2 了。

6.3.4 配置 IP 地址

对于μHammer3550 交换机，要求在一台交换机中，不同 VLAN 必须配置成不同子网段的 IP Address。配置 IP 地址，利用如下命令：

【命令格式】config vlan <name> ipaddress <A.B.C.D/M>

config vlan <name> ipaddress <A.B.C.D> <A.B.C.D>

【参数说明】<name>为所要配置的 VLAN 的名称，<A.B.C.D>为给该 VLAN 配置的 IP 地址，M 为子网掩码数。或者利用第二个命令的格式，输入点分十进制形式的掩码。

【配置实例】给缺省 VLAN default 配置一个 IP 地址 192.168.0.232，子网掩码数为 24，键入命令：

```
Harbour(config)#config vlan default ipaddress 192.168.0.232/24
```

或者，键入命令：

```
Harbour(config)#config  vlan  default  ipaddress  192.168.0.232
  255.255.255.0
```

6.3.5 VLAN 的 Tag 值范围

μHammer3550-24/μHammer3550-48 的 VLAN 的 Tag 值要求在 1-4094 范围之间。

6.4 配置 VLAN

这一小节主要讲述在交换机上配置 VLAN 相关的命令。配置 VLAN 包括以下几步：

1．创建 VLAN 并给该 VLAN 取名。

2．如果需要的话给该 VLAN 分配 IP 地址和子网掩码。

3．给 VLAN 指定一个 Tag（或者使用创建时系统分配的 Tag）。

4．在 VLAN 中加入端口。当您加入端口时可以指定是否使用 802.1Q tag。

表 6-1HammerOS 的 VLAN 配置命令表

命令	描述
create vlan <name>	创建一个 VLAN
config vlan <name> ipaddress <A.B.C.D/M>	配置名为<name>的 VLAN 的 IP 地址和网络掩码长度
config vlan <name> ipaddress <A.B.C.D> <A.B.C.D>	配置名为<name>的 VLAN 的 IP 地址和网络掩码
config vlan <name> tag <1-4094>	指定 VLAN 的 tag 即 VLANID
config vlan <name> [add|delete] port <portlist> [tagged|untagged]	在 VLAN 中增加或删除端口，并设置该端口是 tagged 还是 untagged

6.4.1 配置 VLAN 举例

以下的例子是在µHammer3550-48 上创建了一个名为 development 的 VLAN，给该 VLAN 分配 IP 地址 202.106.15.3 和子网掩码 255.255.255.0，然后加入端口 3，6，17-20，并指定端口为 untagged 模式。

```
Harbour(config)#create vlan development
Harbour(config)#config vlan development ipaddress 202.106.15.3
  255.255.255.0
Harbour(config)#config vlan development add port 3,6,17-20 untagged
```

又如，在µHammer3550-48 交换机上，创建了一个名为 video 的 Tag-Based VLAN，分配给该 VLAN 的 VLANID 是 128。把端口 4 至端口 8 加入该 VLAN 并设为 tagged 模式。

```
Harbour(config)#create vlan video
Harbour(config)#config vlan video tag 128
Harbour(config)#config vlan video add port 4-8 tagged
```

6.4.2 删除 VLAN

【命令格式】delete vlan [<name>|all]

【使用指导】选择 name ，删除指定的 vlan，选择 all 删除所有的 vlan(default 除外)。删除一个 VLAN 后，该 VLAN 的 untagged 模式的端口将被以 untagged 模式放回缺省 VLAN default 中。

【命令模式】配置模式

6.4.3 删除 VLAN 的 IP 地址

【命令格式】no vlan <name> ip

【命令模式】配置模式

【配置实例】删除 vlan market 的 IP 地址

```
Harbour(config)#no ip-vlan market
```

6.4.4 显示 VLAN 配置信息

【命令格式】show vlan {<name>}*1

【使用指导】name 可以输入也可以不输入。当输入 name 的时候，就只显示这个 name 的 VLAN 的信息。当不输入 name 的时候，显示当前交换机中的所有 VLAN 的信息。show 命令所显示的 VLAN 信息包括以下内容：

- VLAN 名字（VLAN name）
- VLANID
- IP 地址
- 属于该 VLAN 的 tagged 模式的端口
- 属于该 VLAN 的 untagged 模式的端口

【配置实例】创建了一个 VLAN development，显示 VLAN 的配置信息，键入命令：

```
Harbour(config)#show vlan development

VLAN ID          : 2046
Name             : development
IP Address        : 202.106.15.3 /24
MAC address       : 10:82:c3:45:11:22
Tagged Ports      :
Untagged Ports     :  3  6  17  18  19  20
```

6.5 VLAN 端口隔离

 **此部分内容仅适用于μHammer3550-24 交换机。**

6.5.1 VLAN 端口隔离概述

VLAN 端口隔离用以限制 VLAN 内各端口之间的访问操作，VLAN 内每个端口只能和上行端口通信，相互之间隔离，不能相互访问。上行口为普通工作模式，ingress 包按普通方式转发。VLAN 的端口隔离配置必须遵循以下规则：

1. Default VLAN 不可配置端口隔离
2. VLAN 上行端口不支持 Load sharing

3. VLAN 上行端口不支持 mirrored_to_port

4. VLAN 的上行端口不能从 VLAN 中删除

5. 端口隔离的 VLAN 不支持基于 VLAN 的 QoS

6.5.2 创建 VLAN 端口隔离

【命令格式】config vlan <name> uplink_port <portno>

【使用指导】为 VLAN 设置上行端口，该端口为 VLAN 成员端口。一个 VLAN 配置了上行端口后，该 VLAN 内每个端口只能和上行端口通信，相互之间隔离，不能相互访问。

【参数说明】参数<name>为 VLAN 名称；portno 为上行口端口号。

【配置实例】

```
Harbour(config)#create vlan iso_vlan
Harbour(config)#config vlan iso_vlan add port 1,2,3 untagged
Harbour(config)#config vlan iso_vlan uplink_port 1
```

此时端口 1 为 vlan iso_vlan 的上行端口， vlan iso_vlan 的其他成员端口 2、3 之间不能访问，只能各自与上行口通信。

注意：当 VLAN 配置了上行端口时，show vlan 命令中会有所反映，例如：

```
Harbour(config)#show vlan iso_vlan

VLAN ID       : 2046
Name          : iso_vlan
VLAN Type     : Normal
MAC address   : 00:05:3b:80:00:01
Uplink Port   : 1
Tagged Ports  :
Untagged Ports : 1  2  3
```

6.5.3 删除 VLAN 端口隔离

【命令格式】no vlan <name> uplink_port

【命令作用】取消 VLAN 端口隔离配置。

【参数说明】参数 name 为 VLAN 的名称。

【配置实例】

```
Harbour(config)#no vlan iso_vlan uplink_port
```

第7章 生成树协议协议

本章包括以下内容

- STP 协议介绍、相关配置及显示 STP 状态
- RSTP 协议介绍、相关配置及显示 RSTP 状态

7.1 STP

Hammer 交换机支持 IEEE802．1d 标准的 STP 协议，它提供了网络的动态冗余切换机制。STP 使您能在网络设计中部署备份线路，并且保证：

- 在主线路正常工作时，备份线路是关闭的。
- 当主线路出现故障时自动使能备份线路，切换数据流。

7.1.1 STP 相关配置

使能或关闭 STP

Hammer 交换机中 STP 缺省状态是关闭的。使能或关闭指定的 STP，利用命令：

config stpd default [enable | disable]

如果键入 enable，表示 STP 有效，如果键入 disable，则表示 STP 无效。

例如：使能 STP，在配置模式下，键入命令：

config stpd default enable

使能或关闭指定 STP 的端口

Hammer 交换机中所有端口默认都是参与 STP 计算的。使能或关闭指定的 STP 端口，在配置模式下，键入命令：

config stpd default port [<portlist>|all] [enable|disable]

其中<portlist>|all 表示所要操作的端口列表，all 表示对所有端口进行操作；如果键入 enable，表示使该端口的 stp 有效，如果为 disable，则无效。

例如：使能指定端口 10 的 STP 功能，在配置模式下，键入命令：

config stpd default port 10 enable

配置指定 STP 的参数

一旦运行某个指定 STP 的 STP 协议后，您可能需要根据具体的网络结构调整该 STP 的一些参数。以下的 STP 协议参数可以在 Hammer 交换机中调整：

- Bridge Priority
- Hello Time
- Forward Delay
- Max Age

另外每个端口上有以下参数可以调整：

- Path Cost
- Port Priority

配置运行 STP 协议时本交换机的优先级

设置运行 STP 协议时本交换机的优先级。利用命令：

config stpd default priority <0-65535>

优先级的取值范围是 0-65535，缺省值为 32768。优先级数值越低，越有可能成为网络中的根桥（Root Bridge）。优先级值为 0 代表了最高的优先级。

例如：设置运行 STP 协议时本交换机的优先级为 2000，键入命令：

config stpd default priority 2000

配置根桥交换机发送 BPDU 的时间间隔

设置当本交换机被选为根桥时发送 BPDU 的时间间隔，利用命令：

config stpd default hellotime <1-10>

HelloTime 的取值范围是 1-10，单位为秒，缺省值是 2 秒。

例如：设置当本交换机被选为根桥时发送 BPDU 的时间间隔为 5 秒，键入命令：

config stpd default hellotime 5

**注意：HelloTime 必须小于等于 ForwardDelay-2**

配置根桥交换机端口状态切换的时间间隔

设置当本交换机被选为根桥时端口状态切换的时间间隔，利用命令：

config stpd default forwarddelay <4-30>

ForwardDelay 的取值范围是 4-30，单位秒，缺省值为 15 秒。

例如：设置当本交换机被选为根桥时端口状态切换的时间间隔为 20 秒，键入命令：

config stpd default forwarddelay 20

**注意：ForwardDelay 的时间必须大于等于 HelloTime+2**

配置 BPDU 报文老化的最长时间间隔

设置 BPDU 报文老化的最长时间间隔，如果收到超过这个时间的 BPDU 报文，就直接丢弃。利用命令：

config stpd default maxage <6-40>

MaxAge 的取值范围是 6-40，单位为秒，缺省值为 20 秒。

例如：设置 BPDU 报文老化的最长时间间隔为 30 秒，键入命令：

config stpd default maxage 30

**注意：Maxage 的时间必须大于等于 2*(HelloTime + 1)，小于等于 2*(ForwardDelay – 1)**

配置参与 STP 计算的端口的优先级

配置参与 STP 计算的端口的优先级，利用命令：

config stpd default port [<portlist> | all] priority <0-255>

其中，<portlist>表示对指定端口进行操作，all 表示对所有端口进行操作。端口优先级的取值范围是 0-255，缺省值是 128。优先级数值越低，端口越容易成为根端口（Root Port），优先级值为 0 代表了最高的优先级。

例如：设置参与 STP 计算的端口 10 的优先级为 120，键入命令：

config stpd default port 10 priority 120

配置参与 STP 计算端口的路径开销

配置参与 STP 计算端口的路径开销，利用命令：

config stpd default port [<portlist> | all] cost <1-65535>

其中，<portlist>表示对指定端口进行操作，all 表示对所有端口进行操作。取值范围是 1-65535，HammerOS 根据端口的当前速度设置不同的缺省值：

- 10Mbps 端口缺省值为 100

- 100Mbps 端口缺省值为 19
- 1000Mbps 端口缺省值为 4

例如：设置参与 STP 计算端口的路径开销为 200，键入命令：

config stpd default port 10 cost 200

7.1.2 显示 STP 状态

显示 STP 的状态

STP 的显示内容包括：

- BridgeID
- Root BridgeID
- STP 的各种配置的参数

利用命令：show stpd default

例如：显示 STP 状态信息，键入命令：show stpd default。信息显示如下：

```
 STP Domain default information
----------------------------------------------------------
-- Designated Root Info --
Priority             :  32768
Mac address          :  00: 05: 3b: 00: 04: 90
Max Age              :  30
Hello Time           :  5
Forward Delay        :  20
-- STP Domain Config Info --
Priority             :  32768
Mac address          :  00: 05: 3b: 00: 04: 90
Root Path Cost       :  200
Root Port            :  10
Bridge Max Age       :  30
Bridge Hello Time    :  5
```

```
Bridge Forward Delay:  20
----------------------------------------------------------
```

显示端口的 STP 状态

端口的 STP 显示内容包括：

- 端口状态
- Designated port
- 端口的各种配置参数

利用下面的命令：

show stpd default port [<portlist> | all]

其中，<portlist>表示对指定端口进行操作，all 表示对所有端口进行操作。

例如：显示端口 10 的 STP 状态，键入命令：

show stpd default port 10

信息显示如下：

```
-------------------------------------------------------------------------
Port 10 's Spanning Tree Protocol Information
Port Join STP Domain default 's Calculate
-- Port Info --
Port id                 :  18
Priority                :  120
State                   :  Disable
Path Cost               :  100
Designated Cost         :  0
-- Designated Port --
Port id                 :  18
Priority                :  128
-- Designated Root --
Priority                :  32768
Mac address             :  00: 05: 3b: 00: 04: 90
```

```
-- Designated Bridge --
Priority            :  32768
Mac address         :  00：05：3b：00：04：90
-------------------------------------------------------------------------
```

7.1.3 STP 的配置命令列表

表 7-1 STP 配置命令列表

命令	解释
config stpd default [enable | disable]	使能或关闭 STP
config stpd default priority <0-65535>	设置运行 STP 协议时本交换机的优先级。 优先级的取值范围是 0-65535，缺省值为 32768。 优先级数值越低，越有可能成为网络中的根桥（Root Bridge）。优先级值为 0 代表了最高的优先级。
config stpd default hellotime <1-10>	设置当本交换机被选为根桥时发送 BPDU 的时间间隔。 HelloTime 的取值范围是 1-10，单位为秒，缺省值是 2 秒。
config stpd default forwarddelay <4-30>	设置当本交换机被选为根桥时端口状态切换的时间间隔。 ForwardDelay 的取值范围是 4-30，单位秒，缺省值为 15 秒。
config stpd default maxage <6-40>	设置 BPDU 报文老化的最长时间间隔，收到超过这个时间的 BPDU 报文，就直接丢弃。 MaxAge 的取值范围是 6-40，单位为秒，缺省值为 20 秒。
config stpd default port [<portlist>|all] [enable|disable]	指定参与 STP 协议计算的端口。
config stpd default port [<portlist> | all] priority <0-255>	配置参与 STP 计算的端口的优先级。 端口优先级的取值范围是 0-255，缺省值是 128。 优先级数值越低，端口越容易成为根端口（Root Port），优先级值为 0 代表了最高的优先级。

config stpd default port [<portlist> | all] cost <1-65535>	配置参与 STP 计算端口的路径开销。 取值范围是 1-65535，HammerOS 根据端口的当前速度设置不同的缺省值： 10Mbps 端口缺省值为 100 100Mbps 端口缺省值为 19 1000Mbps 端口缺省值为 4
show stpd default	显示 STP 状态信息
show stpd default port [<portlist> | all]	显示端口 STP 状态信息

7.2 RSTP

RSTP 协议是依据 IEEE802.1w 标准，对 STP 802.1d 协议进行改进后的协议，它提供了网络的动态冗余切换机制，并在 P2P（非共享）链路上，能够进行端口状态的快速切换。RSTP 协议使得网络设计中可以部署备份线路，并保证在主线路正常工作时，备份线路关闭；而在主线路出现故障时，能自动快速地使能备份线路，切换数据流。

7.2.1 配置 RSTP

在交换机上配置 RSTP 包含以下内容：

- 使能或者关闭交换机 RSTP 功能
- 使能或者关闭端口的 RSTP 功能
- 配置指定的 RSTP 参数

使能或者关闭交换机的 RSTP 功能

Hammer 交换机中 RSTP 功能是默认关闭的。使能或者关闭 RSTP 功能，在配置模式下，键入命令：

config spanning-tree [enable | disable]

如果键入 enable， 表示使能 RSTP；如果键入 disable， 表示关闭 RSTP 功能。

例如：使能 RSTP，在配置模式下，键入命令：

config spanning-tree enable

使能或者关闭端口的 RSTP 功能

Hammer 交换机中所有端口都是默认参与 RSTP 计算的。使能或者关闭端口的 RSTP 功能，在配置模式下，键入命令：

Config spanning-tree port <port> [none-stp] [yes | no]

其中<port>表示所要操作的端口的端口号；如果参数为 yes，则表示关闭该端口的 RSTP 功能，如果参数为 no，表示使能该端口的 RSTP 功能。

例如：关闭指定端口 10 的 RSTP 功能，在配置模式下，键入命令：

config spanning-tree port 10 none-stp yes

配置指定的 RSTP 参数

一旦运行了 RSTP 协议，您可能需要根据具体的网络结构调整 RSTP 的一些参数：

- Bridge Priority
- Hello Time
- Forward Delay
- Max Age
- Force-version

另外，每个端口还有以下参数可以调整：

- Path Cost
- Port Priority
- P2P 属性
- Edge 属性

配置运行 RSTP 协议时本交换机的优先级

设置运行 RSTP 协议时本交换机的优先级，利用命令：

Config spanning-tree priority <0-61440>

交换机优先级的范围为 0-61440，缺省值为 32768。交换机优先级数值越低，越有可能成为网络中的根桥（Root Bridge）。优先级值为 0 代表了最高的优先级。交换机的优先级数值应该是 4096 的倍数。例如：设置运行 RSTP 协议时本交换机的优先级为 8192，键入命令：

config spanning-tree priority 8192

配置本交换机发送 BPDU 的时间间隔

设置本交换机发送 BPDU 的时间间隔，利用命令：

Config spanning-tree hello-time <1-10>

HelloTime 的取值范围是 1－10，单位为秒，缺省值为 2 秒。例如：设置本交换发送 BPDU 的时间间隔为 4 秒，键入命令：

config spanning-tree hello-time 4

配置本交换机端口状态切换的时间间隔

设置本交换机端口状态切换的时间间隔，利用命令：

Config spanning-tree forward-delay <4-30>

ForwardDelay 的取值范围是 4－30，单位为秒，缺省值为 15 秒。例如，设置本交换机端口状态切换的时间间隔为 10 秒，键入命令：

config spanning-tree forward-delay 10

注意：Hello-time， Max-Age 和 Forward-Delay 的配置值必须满足以下关系：

2*(Hello-time + 1) <= Max-Age <= 2*(Forward-Delay - 1)

配置 BPDU 报文老化的最长时间间隔

设置 RSTP BPDU 报文老化的最长时间间隔，如果收到超过这个时间的 BPDU 报文，就直接丢弃。利用命令：

Config spanning-tree maximum-age <6-40>

Maximum-age 的取值范围是 6－40，单位为秒，缺省值为 20 秒。例如，设置 RSTP BPDU 报文老化的最长时间间隔为 30 秒，键入命令：

config spanning-tree maximum-age 30

注意：Hello-time， Max-Age 和 Forward-Delay 的配置值必须满足以下关系：

2*(Hello-time + 1) <= Max-Age <= 2*(Forward-Delay - 1)

配置参与 RSTP 计算的端口的优先级

配置参与 RSTP 计算的端口的优先级，利用命令：

Config spanning-tree port <port> [priority] <0-240>

端口优先级的取值范围是 0－240，端口优先级的值应该是 16 的倍数，其缺省值是 128。优先级数值越低，端口越容易成为根端口（Root Port），优先级值为 0 代表了最高的优先级。例如，设置参与 RSTP 计算的端口 10 的优先级为 96，键入命令：

config spanning-tree port 10 priority 96

配置参与 RSTP 计算的端口的路径开销

配置参与 RSTP 计算的端口的路径开销，利用命令：

Config spanning-tree port <port> [path-cost] [auto | <1-200000000]

端口的路径开销的取值范围是 1-200000000。 用户可以自己设定端口开销，也可以使用系统的默认设置，即 auto。 端口路径开销设置为 auto 时，由 RSTP 自动检测端口类型，从而决定参加 RSTP 计算的端口的端口路径开销。

- 10Mbps 端口缺省值为 2000000
- 100Mbps 端口缺省值为 200000
- 1000Mbps 端口缺省值为 20000

例如，设置参与 RSTP 计算的端口 10 的路径开销为 300000，键入命令：

config spanning-tree port 10 path-cost 300000

配置交换机的 STP 协议的版本

为了兼容 IEEE 802.1d 标准规定的 STP 协议，在 RSTP 运算中，用户可以设置交换机运行 802.1d 的 STP 协议，利用命令：

config spanning-tree [force-version] [0 | 2]

当取 force-version 的值为 2 时，交换机运行 RSTP 协议；当取 force-version 的值为 0 时，交换机运行老的 STP 协议。其缺省值为 2，即交换机默认执行 RSTP 协议。例如，设置交换机运行 IEEE 802.1d STP 协议，键入命令：

config spanning-tree force-version 0

选择 STP 协议的工作模式

用户可以选择运行 802.1d STP 协议或者 802.1w RSTP 协议，利用命令：

config spanning-tree mode [stp|rstp]

stp 表示 802.1d STP 协议，rstp 表示 802.1w RSTP 协议。如用户希望运行 RSTP 时，键入命令：

config spanning-tree mode rstp

检测是否有运行 802.1d STP 的桥相连

当 RSTP 工作在 STP 兼容模式下的时候，检查周围是否还有运行 802.1d STP 的桥，利用命令：

config spanning-tree mcheck yes

**注意：由于是一次性的功能，不产生长期效果，此功能不能在 show run 中进行保存。**

配置端口的 P2P 属性：

配置端口的 P2P 属性，利用命令：

Config spanning-tree port <port> p2p [yes | no | auto]

可以取值 yes， no， auto。其缺省值为 auto， RSTP 会自动检测端口的 P2P 类型。只有在 P2P 为真的情况下，才可能利用 RSTP 运算， 进行端口状态的快速转移。例如，设置端口 10 的 P2P 属性为真，键入命令：

config spanning-tree port 10 p2p yes

配置端口的 edge 属性：

配置端口的 Edge 属性，利用命令：

config spanning-tree port <port> [edge] [yes | no]

edge 属性可以取值 yes， no，其缺省值为 no。当交换机的这个端口直接与主机相连，或者这个端口再不与其他交换机连接的情况下，可以设置端口的 edge 属性为 yes，这样可以使得端口可以进行快速的状态转换。例如，设置端口 10 的 edge 属性为真，键入命令：

config spanning-tree port 10 edge yes

7.2.2 显示 RSTP 状态

显示交换机 RSTP 的状态

RSTP 的显示内容：

- BridgeID
- Root BridgeID
- RSTP 的各种配置的参数

显示 RSTP 状态的内容，利用命令：show spanning-tree。例如，在交换机上，显示 RSTP 状态信息，键入命令：

show spanning-tree

信息显示如下：


```
----------------------SPANNING TREE infomation in STP domain 2047 ----------------------
-- Designated Root Info --
Priority                : 133726292
MAC address             : 00:05:3b:04:00:50
Designated Port   ID    : 0/13
Max Age                 : 20
Hello Time              : 2
Forward Delay           : 15

-- STP Domain Config Info --
Priority                : 133726272
MAC address             : 22:22:22:22:22:22
Root Port               : 0/18
Root Path Cost          : 200000
Bridge Max Age          : 20
Bridge Hello Time       : 2
Bridge Forward Delay : 15
Bridge ForceVersion     : 2

--------------All ports infomation in STP domain 2047 ------------------------
 Num pri     path--cost role span-state    lnk   p2p   edg   pen dcost     designated root id
 0/24 128      2000000    Dis Discarding    N     N     N     N 200000 32768:00053b040050
 0/23 128      2000000    Dis Discarding    N     N     N     N 200000 32768:00053b040050
 0/22 128      2000000    Dis Discarding    N     N     N     N 200000 32768:00053b040050
 0/21 128      2000000    Dis Discarding    N     N     N     N 200000 32768:00053b040050
 0/20 128      2000000    Dis Discarding    N     N     N     N 200000 32768:00053b040050
 0/19 128      2000000    Dis Discarding    N     N     N     N 200000 32768:00053b040050
 0/18 128       200000 Root Forwarding      Y     Y     N     N 200000 32768:00053b040050
 0/17 128      2000000    Dis Discarding    N     N     N     N 200000 32768:00053b040050
 0/16 128      2000000    Dis Discarding    N     N     N     N 200000 32768:00053b040050
```

```
0/15 128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/14 128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/13 128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/12 128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/11 128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/10 128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/9    128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/8    128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/7    128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/6    128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/5    128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/4    128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/3    128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/2    128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050
0/1    128      2000000    Dis Discarding    N    N    N    N 200000 32768:00053b040050

-----------------------------------------------------------------------------
```

显示端口的 RSTP 状态

端口的 RSTP 状态的显示内容：

- 端口状态
- 端口配置参数

显示端口 RSTP 状态，利用下面的命令：show spanning-tree port <port>。其中，<port>表示指定端口的端口号。例如，在交换机上，显示端口 10 的 STP 状态，键入命令：

show spanning-tree port 10

信息显示如下：

```
----- port 0/0 infomation in STP domain 2047 -----
Num pri    path--cost   role span-state   lnk   p2p   edg   pen dcost   designated root id
```

0/10 128 2000000 Dis Discarding N N N N 200000 32768:00053b040050

7.2.3 RSTP 的配置命令列表

表 7-2RSTP 配置命令列表

命令	解释
config spanning-tree [enable | disable]	使能或关闭 RSTP 功能
config spanning-tree priority <0-61440>	配置桥的优先级（4096 的倍数）
config spanning-tree maximum-age <6-40>	配置 BPDU 的老化时间
config spanning-tree hello-time <1-10>	配置桥的 hello-time
config spanning-tree forward-delay <4-30>	配置桥的 forward-delay
config spanning-tree [force-version] [0 | 2]	配置 RSTP 协议的版本
config spanning-tree mcheck yes	检测是否有运行 802.1d STP 的桥相连
config spanning-tree port <port> [path-cost] [auto | <1-200000000]	配置端口的路径开销
config spanning-tree port <port> [priority] <0-240>	配置端口的优先级(16 的倍数)
config spanning-tree port <port> [none-stp] [yes | no]	配置端口使能或关闭 RSTP 功能
config spanning-tree port <port> p2p [yes | no | auto]	配置端口的 P2P 属性
config spanning-tree port <port> [edge] [yes | no]	配置端口的 edge 属性
show spanning-tree	查看桥的 RSTP 的配置状态
show spanning-tree port <port>	查看端口的 RSTP 的配置状态

第8章 IGMP Snooping

IGMP（Internet Group Management Protocol）网络组管理协议是 IP 协议组中的一部分，用来支持和管理主机与组播路由器之间的 IP 组播。组播允许进行资源发现，使网络负载减到最小，在网上实现数据的有效传输。

IGMP Snooping 用来监听主机与路由器之间的 IGMP 报文，并对监听到的 IGMP 报文进行处理。IGMP Snooping 使交换机能够跟踪与之物理相连的网络上每个组的成员。它在主机和直接邻接的组播路由器间运行，管理组成员关系。

8.1 启动 IGMP Snooping

启动 IGMP，在配置模式下，键入命令：

```
service igmp snooping enable
```

8.2 配置 IGMP Snooping 超时时间间隔

1．配置路由器端口的超时时间间隔，利用命令：

```
config igmp snooping router_timeout <10～2147483647>
```

router_timeout ：表示要调整的是路由器端口的时间间隔，默认值为 260 秒。

10~2147483647 ：表示调整路由器端口的超时范围。

2．配置主机端口的超时时间间隔，利用命令：

```
config igmp snooping host_timeout <10～2147483647>
```

host_timeout ：表示要调整的是主机端口的时间间隔，默认值为 260 秒。

10~2147483647 ：表示超时时间范围。

例如，配置接口，router_timeout = 500 秒，host_timeout = 600 秒，键入命令：

```
Harbour(config)#config igmp snooping router_timeout 500

Harbour(config)#config igmp snooping host_timeout 600
```

使用以下命令可以查看主机和路由器端口的超时时间间隔：

```
show igmp snooping summary
```

例如：

```
Harbour(config)#show igmp snooping summary

---------- igmp snooping summary ----------
Router timeout                   260s(D)
Host   timeout                   260s(D)
Total    group                   0
Max     group                    255
-------------------------------------------
D: default.
```

8.3 清除 IGMP Snooping 信息

清除某个 VLAN 或所有 VLAN 中的组成员，在配置模式下，利用命令：

```
clear igmp snooping vlan [name|all]
```

其中，参数<name>为指定 VLAN 的名称，all 代表所有的 VLAN。

例如，清除 default 中的所有组成员关系，在配置模式下，键入命令：

```
Harbour(config)#clear igmp snooping vlan default
```

8.4 关闭 IGMP Snooping 功能

关闭 IGMP，在配置模式下，键入命令：

```
service igmp snooping disable
```

8.5 显示 IGMP Snooping 信息

显示指定 VLAN 中或所有 VLAN 中的组成员信息，在配置模式下，利用命令：

```
show igmp snooping vlan <name>
```

其中，参数<name>为指定 VLAN 的名称，当<name>为 all 时，表示所有的 VLAN。

例如，显示 default 中的所有组成员关系，键入命令：

```
show igmp snooping vlan default
```

8.6 IGMP Snooping 命令表

表 8-1 IGMP Snooping 配置命令表

命令	描述
Service igmp-snooping [enable|disable]	启用/禁止 IGMP Snooping 功能
config igmp snooping router_timeout <10～2147483647>	指定路由器超时的时间间隔（默认值 260 秒）
config igmp snooping host_timeout <10～2147483647>	指定主机超时的时间间隔（默认值 260 秒）
clear igmp snooping vlan <name>	清除某个 VLAN 中或所有 VLAN 中的组成员信息列表，当 name 为 all 时表示全部的 VLAN
show igmp snooping timer	显示主机和路由器端口的超时时间间隔
show igmp snooping vlan <name>	显示某个 VLAN 中或所有 VLAN 中的组成员

第9章 QoS

9.1 QoS 概述

9.1.1 概述

QoS（Quality of Service）指 IP 的服务质量，也就是 IP 数据流通过网络时的性能，它的目的是向用户业务提供端到端的服务质量保证。它有一套度量指标，包括业务可用性、延迟、可变延迟、吞吐量和丢包率。QoS 在可预测、可测量性方面比传统 IP 有了很大提高，基本解决了商业用户的需求，因而可以吸引更多的商业用户，形成一个新的利润增长点，带来可增值的业务种类。另外， QoS 还带来了更高效的带宽使用率等。因此可以说 QoS 将是今后一段时间促进 IP 网络增长的关键技术。

不同的应用有不同的 QoS 需求，如语音、图像对抖动和时延敏感，则要求保证带宽和高的优先级；数据和文件传输则对时延不敏感，则可在保证带宽的前提下采用较低的优先级。µHammer3550-24/µHammer3550-48 最多支持 4 个优先级队列。支持严格优先级 SP（Strict Priority）和加权轮循优先级 WRR（Weighted Round Robin）两种调度策略。

- 严格优先级调度机制SP：严格按优先级的高低从队列中提取转发数据，高优先级队列的数据没有清空之前，不转发低优先级队列中的数据。
- 加权轮询调度机制WRR：可以设置以包为单位的Low，Normal，Medium，High的权重比例，按比例轮循4个队列。

目前版本的 QoS 功能只支持 CoS 队列优先级调度和 802.1p 及基于 MAC、PORT、VLAN、ACL 的优先级之间的映射。CoS 队列优先级调度可以分为三个过程：对数据包进行分类；指定不同的优先级队列；得到不同的服务质量（按优先级转发）。

9.1.2 QoS 优先级顺序

配置 QoS 命令优先级的顺序从低到高为：基于 MAC < PORT 重映射< 基于 VLAN < 基于 ACL。

所以如果先配有优先级高的 QoS 策略，再配置低的策略，低的策略将不会发生作用，所以建议在配置 QoS 之前需要全局考虑，避免实际功能与设计中的不一样。

9.1.3 区别服务（DiffServ）

µHammer3550-24/µHammer3550-48 的 QoS 功能提供针对 IPv4 包的区别服务（DiffServ），该服务主要应用 IPv4 报头字段中的 DSCP 域，可以向用户提供以下服务：

- 重写IPv4数据流中的DSCP值
- 根据IPv4数据包中的DSCP值，映射到本地的转发优先级队列中，实现转发优先排序

目前版本支持的 DiffServ 方式有以下三种：

- 基于PORT的DiffServ

- 基于VLAN的DiffServ
- 基于ACL的DiffServ

9.1.4 服务类型（ToS）

μHammer3550-24/μHammer3550-48 的 QoS 可以根据以下规则重写 IPv4 数据流的 ToS 域：

- 基于VLAN重写ToS域
- 基于ACL重写ToS域

μHammer3550-24/μHammer3550-48 支持基于端口（入口和出口）的带宽限制，百兆口粒度为 1M，千兆口粒度为 8 兆。

9.2 QoS 相关配置

9.2.1 使能或者禁止 QoS 服务

使能/禁止 QoS 功能。通过设置 CoS 优先级到相应队列的映射关系来实现。

【命令格式】service qos [enable|disable]

【使用指导】初始化状态下 8 个 802.1p 优先级映射到唯一的 0 号 CoS 队列。如果选择 enable 则启动 4 个 CoS 队列，8 个 802.1p 分别映射到相应的 CoS 队列；如果选择 disable 则禁止 QoS 功能，与 QoS 相关的命令不可用。

【命令模式】配置模式

9.2.2 CoS 优先级调度策略配置

CoS 优先级调度策略的配置，利用如下命令：

【命令格式】config WRR-queue bandwidth <low,normal,medium,high>

【使用指导】4 个 CoS 优先级队列 0、1、2、3 分别表示 low、normal、medium、high。

如果采用严格轮循方式（SP）则执行命令：config WRR-queue bandwidth 0,0,0,0。这样只有在高优先级的队列清空以后，低优先级队列中的包才转发。

如果采用加权轮循方式（WRR）执行命令：config WRR-queue bandwidth 1,2,3,4。Low：Norma：Medium：High 的权重比例关系为 1：2：3：4，即每一次轮循从 High 队列中取 4 个包；从 Medium 队列中取 3 个包；从 Norma 队列中取 2 个包；从 Low 队列中取 1 个包。这四个参数的取值范围都是 1-255。

【命令模式】配置模式

查看 CoS 优先级配置，利用以下命令：

【命令格式】show wrr-queue

【使用指导】显示 4 个优先级队列与权重的对应关系

【配置模式】只读或者配置模式

【配置实例】配置加权轮循权重为 1,2,3,4，则有如下显示：

```
Harbour(config)#config WRR-queue bandwidth 1,2,3,4
Harbour(config)#show wrr-queue

-------- QoSQueue -------- WRR value --------
--------  Low     --------  1    -----------
--------  Normal  --------   2    -----------
--------  Medium  --------   3    -----------
--------  High    --------   4    -----------
```

9.2.3 802.1p 优先级到 CoS 队列的映射关系配置

配置 802.1p 的优先级到 CoS 的映射关系，利用命令：

【命令格式】config priority <0-7> qosqueue [Low|Normal|Medium|High]

【使用指导】通过设置 CoS_SEL 寄存器的相应位来指定 802.1p 优先级到 CoS 队列的映射关系。

【命令模式】配置模式

9.2.4 查看 802.1p 优先级到 CoS 队列的映射关系配置

可以用如下命令查看 802.1p 优先级到 CoS 队列的映射关系配置。

【命令格式】show dot1p-QosQueue-mapping

【配置实例】

没有配置 802.1p 优先级到 CoS 队列的映射关系时，我们查看一下它们的映射关系。

```
Harbour(config)#show dot1p-qosqueue-mapping

--------Dot1p Priority--------------QoS Queue ---------
---------     0     --------  Low     --------
---------     1     --------  Low     --------
---------     2     --------  Normal   --------
---------     3     --------  Normal   --------
---------     4     --------  Medium   --------
---------     5     --------  Medium   --------
---------     6     --------  High    --------
---------     7     --------  High    --------
```

下面我们把 802.1p 优先级 7 映射到表示为 Low 的 0 号 CoS 队列。我们再查看一下他们的映射关系。

```
Harbour(config)#config priority 7 qosqueue low
```

```
Harbour(config)#show dot
Harbour(config)#show dot1p-qosqueue-mapping

--------Dot1p Priority-----------QoS Queue ---------
---------     0     --------    Low      --------
---------     1     --------    Low      --------
---------     2     --------    Normal    --------
---------     3     --------    Normal    --------
---------     4     --------    Medium    --------
---------     5     --------    Medium    --------
---------     6     --------    High      --------
---------     7     --------    Low      --------
```

9.2.5 基于 MAC 的优先级配置

【命令格式】create fdbentry <mac_address> vlan <name> port <portlist> {priority <0-7>}*1

【使用指导】为创建静态 FDB 表项的命令添加优先级参数，则以此 MAC 地址为源 MAC 的数据包会根据配置的 802.1p 优先级来选择 CoS 队列。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#create fdb 001122334455 vlan default port 5 priority
  7
Harbour(config)#show qos mac

****************************MAC
  Qos******************************
MAC address         Port  VLAN name                 Priority
00:11:22:33:44:55    5    default                     7
```

9.2.6 基于 PORT 的优先级配置

使能或者禁止端口到 802.1p 优先级的重新映射功能，利用如下命令：

【命令格式】config port [<portlist>|all] remap-priority [on|off]

【使用指导】使能/禁止端口对 802.1p 优先级的重新映射功能

【命令模式】配置模式

9.2.7 配置端口到 802.1p 优先级的重新映射

【命令格式】config port [<portlist>|all] remap-priority <0-7>

【使用指导】通过设置相应端口重新映射 priority 的值改变端口对 802.1p 优先级的重新映射。则从此端口接收的数据包根据配置的 802.1p 优先级来选择 CoS 队列。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config port 1 remap-priority on
Harbour(config)#config port 1 remap-priority 6
Harbour(config)#show qos port
```

```
****************************Port
  Qos*******************************
Port: 1's 802.1p priority is 6.
```

9.2.8 基于 VLAN 的优先级配置

【命令格式】config vlan <name> priority <0-7>

【使用指导】通过改变 VLAN 的优先级属性来实现属于某一个 VLAN 的数据流的优先级的重新映射。属于该 VLAN 的数据流的 802.1p 优先级被配置的优先级取代，转发到相应的 CoS 队列。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config vlan test priority 7
Harbour(config)#show qos vlan

****************************VLAN
  Qos*******************************
VLAN: test's 802.1p priority is 7.
```

9.2.9 基于 ACL 的优先级配置

【命令格式】config acl <name> priority <0-7>

【使用指导】通过修改 ACL 策略的优先级属性来实现基于 ACL 的数据流优先级的重新映射。则匹配上该 ACL 策略的数据流的 802.1p 优先级被配置的优先级取代，转发到相应的 CoS 队列。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config acl test priority 6
Harbour(config)#show qos acl

****************************Acl
  Qos*******************************
ACL : test's 802.1p priority is 6.
```

9.3 DiffServ 相关配置

IP 包头中的 ToS（Type Of Service）域代表了相应的服务类型。DiffServ 将 8 位 ToS 字段重新命名，作为 DS (DifferServer)字段，利用前 6 位做为 DSCP（ DifferServer CodePoint）域，这个域的值我们称为 codepoint，交换机可以使用这个域进行包服务类型的区分。在交换机中可以实现根据服务的级别对于包重写 DSCP 域，或者根据 DSCP 域来进行 QoS 的区分，实现区别服务。DiffServ 的配置用于处理 IPv4 首部的 DSCP 域，内容包括：

1. 重写 IPv4 报文首部中的 DSCP 域

- 基于进入特定端口IPv4报文DSCP域的重写

- 基于特定VLAN的IPv4报文DSCP域的重写
- 基于特定ACL的IPv4报文DSCP域的重写

2. 映射不同的 DSCP 值到 802.1p 定义的优先级，使得带有不同的 DSCP 值的 IPv4 报文得到不同的发送优先级别。是否进行优先级映射可由用户选择配置。

DiffServ 功能模块的命令集有一定的配置顺序，建议按以下顺序配置：

1）service qos enable

2）config dscp to-802.1p map codepoint [0-7|8-15|16-23|24-31|32-39|40-47|48-55|56-63] priority <0-7>

3）config dscp enable

4）config dscp to-802.1p [on|off] ，默认打开

9.3.1 使能或者禁止 Differv 服务

【命令格式】config dscp [enable|disable]

【使用指导】启动或关闭 DiffServ 服务，默认启动时同时打开 differv 优先级映射功能。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config dscp enable
```

9.3.2 使能或者禁止 Differv 优先级映射功能

【命令格式】config dscp to-802.1p [on|off]

【使用指导】打开或关闭 DiffServ 优先级映射功能。

on 表示交换机将根据 IPV4 数据流的 DSCP 值，将其映射到不同的本地优先级转发队列中去，从而得到不同级别的发送优先服务。

off 表示交换机不进行优先级映射，具有不同 DSCP 值的 IPV4 数据流在本地的转发优先级没有高低之分。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config dscp to-802.1p on
Harbour(config)#config dscp to-802.1p off
```

9.3.3 配置 Differv 到 802.1p 的映射关系

【命令格式】config dscp to-802.1p map codepoint [0-7|8-15|16-23|24-31|32-39|40-47|48-55|56-63] priority <0-7>

【使用指导】配置 differv 每一段 dscp codepoint 值到 802.1p 优先级的映射关系。默认配置为：

dscp codepoint	802.1pri
0-7	0
8-15	1
16-23	2
23-31	3
32-39	4
40-47	5
48-55	6
56-63	7

【命令模式】配置模式

【配置实例】

Harbour(config)#dscp to-802.1p map codepoint 16—23 priority 2

9.3.4 基于 VLAN 的 DSCP 配置

【命令格式】config vlan <vlanname> dscp <0-63>

【使用指导】配置基于 vlan 的 dscp

【命令模式】配置模式

【配置实例】Harbour(config)#config vlan default dscp 6

【命令格式】no vlan <name> dscp

【使用指导】去除 vlan 的 dscp 属性

【命令模式】配置模式

【配置实例】Harbour(config)#no vlan default dscp

9.3.5 基于 ACL 的 DSCP 配置

【命令格式】config acl <name> dscp <0-63>

【使用指导】配置基于 acl 的 dscp

【命令模式】配置模式

【配置实例】Harbour(config)#config acl acl_1 dscp 24

【命令格式】no acl <name> dscp

【使用指导】去除 acl 的 dscp 属性

【命令模式】配置模式

【配置实例】Harbour(config)#no acl acl_1 dscp

9.3.6 基于 PORT 的 DSCP 配置

【命令格式】config port [<portlist>|all] dscp <0-63>

【使用指导】portlist 端口列表，例如 8-12 表示 8，9，10，11，12 端口。dscp 后面的参数就是给端口配置的 codepoint 的值

【命令模式】配置模式

【配置实例】Harbour(config)#config port 1，3—12，5 dscp 63

【命令格式】no port [<portlist>|all] dscp

【使用指导】去除 port 的 dscp 属性

【命令模式】配置模式

【配置实例】Harbour(config)#no port 4 dscp

9.3.7 查看 DiffServ 的配置信息

【命令格式】show dscp [vlan|acl|port|all]

【使用指导】显示 DiffServ 的配置信息

【命令模式】配置模式

【配置实例】

```
Harbour(config)#show dscp all

-------------VLAN DSCP-------------
VLANName                       DSCP
--------                       ----
v1                              10
-----------------------------------

-------------ACL  DSCP-------------
AclName                        DSCP
-------                        ----
test                            10
-----------------------------------
```

9.3.8 查看 DiffServ 到 8021.p 的映射信息

【命令格式】show dscp map

【使用指导】显示 DiffServ 到 802.1p 的映射信息

【命令模式】配置模式

【配置实例】

```
Harbour(config)#show dscp map

dscp codepoint     802.1pri
0-7               0
8-15              1
16-23             2
23-31             3
```

```
32-39           4
40-47           5
48-55           6
56-63           7
```

9.4 ToS 相关配置

IP 包头中的 ToS（Type Of Service）域代表了相应的服务类型。在交换机中可以使用这个域进行包服务类型的区分，可以根据以下规则来重写该域的值：

- 基于特定VLAN的IPv4报文ToS域的重写
- 基于特定ACL的IPv4报文ToS域的重写

9.4.1 使能或者禁止 ToS 服务

【命令格式】config tos [enable|disable]

【使用指导】启动或关闭 tos 服务。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config tos enable
```

9.4.2 基于 VLAN 的 ToS 配置

【命令格式】config vlan <name> tos_p <1-7>

【使用指导】配置基于 vlan 的 ToS，重写在该 vlan 中转发的 IP 数据的 ToS 域

【命令模式】配置模式

【配置实例】Harbour(config)#config vlan test tos_p 6

【命令格式】no vlan <name> tos_p

【使用指导】去除 vlan 的 tos 属性

【命令模式】配置模式

【配置实例】Harbour(config)#no vlan test tos_p

9.4.3 基于 ACL 的 ToS 配置

【命令格式】config acl <name> tos_p <0-7>

【使用指导】配置基于 ACL 的 tos，重写匹配该 ACL 项的 IP 数据的 tos 域

【命令模式】配置模式

【配置实例】Harbour(config)#config acl acl_1 tos_p 5

【命令格式】no acl <name> top_p

【使用指导】去除 ACL 的 tos 属性

【命令模式】配置模式

【配置实例】Harbour(config)#no acl acl_1 tos_p

9.4.4 查看 ToS 配置信息

【命令格式】show tos_p [vlan|acl|all]

【使用指导】显示 ToS 的配置信息

【命令模式】配置模式

【配置实例】

```
Harbour(config)#show tos all

-------------VLAN ToS-------------
VLANName                    ToS_P
--------                    -----
v1                            3
----------------------------------
-------------ACL  ToS-------------
AclName                      ToS_P
-------                     -----
test                           2
----------------------------------
```

9.5 带宽限制（bandwidth）

9.5.1 配置入口端口的带宽限制

【命令格式】config port [<portlist>|all] bandwidth input <0-127>

【使用指导】配置端口的入口带宽限制。参数<0-127> 指允许的带宽，单位 M（百兆口），8M（千兆口）。

【命令模式】配置模式

【配置实例】Harbour(config)#config port 3 bandwidth input 20

9.5.2 配置出口端口的带宽限制

【命令格式】config port [<portlist>|all] bandwidth output <0-127>

【使用指导】配置端口的出口带宽限制。参数<0-127> 指允许的带宽，单位 M（百兆口），8M（千兆口）。

【命令模式】配置模式

【配置实例】Harbour(config)#config port 3 bandwidth output 20

9.5.3 查看端口的带宽限制信息

【命令格式】show bandwidth port

【使用指导】查看端口的带宽限制信息。

【命令模式】配置模式

【配置实例】Harbour(config)#show bandwidth port 3

9.6 QoS 命令列表

命令	描述
service qos [enable|disable]	使能/禁止 QoS 功能
config WRR-queue bandwidth <low,normal,medium,high>	配置队列加权轮循的权重
show WRR-queue	显示 4 个优先级队列与权重的对应关系
config priority <0-7> qosqueue [Low|Normal|Medium|High]	配置 802.1p 优先级到 COS 队列的映射关系
show dot1p-QosQueue-mapping	显示 802.1p 优先级到 COS 队列的映射关系
create fdbentry <mac_address> vlan <name> port <portlist> {priority <0-7>}	配置 FDB 对 802.1p 优先级的重新映射
config port [<portlist>|all] remap-priority <0-7>	配置相应端口对 802.1p 优先级的重新映射
config vlan <name> priority <0-7>	配置 VLAN 的数据流的优先级的重新映射
no vlan <name> priority	取消已经配置的 vlan 优先级配置信息
config acl <aclname> priority <0-7>	配置 ACL 策略的数据流的优先级的重新映射
no acl <name> priority	取消已经配置的 ACL 优先级配置信息
show qos [port|mac|vlan|acl|all]	显示不同类型的 QoS 优先级配置信息
config tos [enable|disable]	打开或关闭 tos 功能
config vlan <name> tos_p <1-7>	配置基于 vlan 的 Tos
no vlan <name> tos_p	去除基于 vlan 的 Tos 属性
config acl <aclname> tos_p <0-7>	配置基于 acl 的 Tos
no acl <name> top_p	去除基于 acl 的 Tos 属性
show tos_p [vlan|acl|all]	显示 tos 信息

第10章 日志管理

本章主要包括以下内容：

- 日志管理概述
- 日志功能基本配置
- 日志信息存储方式配置
- 日志信息显示方式配置
- 查看日志管理的配置情况
- 日志管理命令列表

10.1 日志管理概述

日志管理主要用来记录整个系统的运行情况以及用户操作行为。完整的日志管理能够帮助管理员及时了解和监控系统的工作情况，并实时记录系统的异常信息。日志信息来源于系统中所有的运行模块，日志系统完成信息的收集、管理、存储和显示。日志信息可以显示到终端 monitor，这种方式主要用于调试和查看系统状态。也可以存储到日志服务器 server，这种方式用于长期跟踪系统的运行情况以及用户的命令行操作行为。

10.2 日志功能基本配置

10.2.1 打开或关闭日志服务

【命令作用】打开或关闭日志服务功能

【命令格式】config syslog [enable|disable]

【参数说明】选择 enable 表示打开日志服务功能；选择 disable 表示关闭日志服务功能

【命令模式】配置模式

【配置实例】打开日志服务功能

```
Harbour(config)#config syslog enable

Successfully changed syslog service to enable
```

10.2.2 配置所要记录的日志信息的类型

【命令作用】配置日志管理是否对某一类型的日志信息进行记录

【命令格式】config syslog type [<name>|all] [enable|disable]

【参数说明】选择 enable 表示对指定类型的信息进行记录；选择 disable 表示不记录。

【命令模式】配置模式

【使用指导】name 为系统中支持的日志类型，可用 show syslog configuration 来查看日志类型，目前支持的类型有：AUTH，BGP，CLI，SYSLOG，DEVCTRL，ARP，DOT1X，NAS，OSPF，

PORT，FDB，RADIUS，RIP，ROUTE，SNMP，STP，SYSTEM，VLAN，WEB，SERVICE，DHCPR 等。all 代表以上支持的所有日志类型。

【配置实例】注册 AUTH 类型的日志信息，日志管理将对 AUTH 类型的日志信息进行记录：

```
Harbour(config)#config syslog type auth enable

Successfully changed syslog type auth to enable.
```

10.2.3 配置所要记录日志信息的最低级别

【命令作用】配置日志管理对某一级别和该级别以上的日志信息进行记录

【命令格式】config syslog lowest-level <0-7>

【命令模式】配置模式

【使用指导】目前支持的日志信息级别从 0 到 7，依次为 EMERG ，ALERT ，CRITERR，CRIT， ERR，WARNING，NOTICE，INFO，DEBUG。

【配置实例】级别 3 和级别 3 以上（即级别 0－3）的日志信息将被记录：

```
Harbour(config)#config syslog lowest-level 3

Successfully changed syslog service lowest-lever level 3 [ERR].
```

10.2.4 打开命令行操作日志记录功能

【命令作用】配置日志管理是否对命令行操作行为进行日志记录

【命令格式】record command-line [enable|disable]

【参数说明】enable 表示对命令行操作进行记录；disable 表示对命令行操作不进行记录。

【命令模式】配置模式

【使用指导】命令行操作的日志信息级别为 6，即 INFO 类型。

【配置实例】允许对命令行操作行为记录日志信息：

```
Harbour(config)#record command-line enable

Successfully changed syslog record CLI to enable.
```

10.2.5 打开或关闭有效用户通过 telnet 登录成功的日志记录功能

【命令作用】配置日志模块是否对有效用户通过 telnet 登录成功进行日志记录

【命令格式】record valid-access [enable|disable]

【参数说明】选择 enable 表示进行日志记录；选择 disable 表示不进行日志记录。

【命令模式】配置模式

【使用指导】命令行操作的日志信息级别为 5，即 NOTICE 类型。

【配置实例】允许对有效用户通过 telnet 登录成功进行日志记录：

```
Harbour(config)#record valid-access enable
```


10.3 日志信息存储方式配置

10.3.1 打开或关闭日志信息保存到日志服务器的功能

【命令作用】配置日志管理是否保存日志信息到日志服务器

【命令格式】config syslog server [enable|disable]

【参数说明】enable 表示保存日志信息到服务器；disable 表示不保存日志信息到服务器。

【命令模式】配置模式

【使用指导】在配置之前，保证日志服务器服务程序已启动。

【配置实例】允许日志保存到日志服务器：

```
Harbour(config)#config syslog server enable

Successfully changed syslog service logto server enable.
Warning: Syslog server config is empty.Please add syslog server.
```

10.3.2 增加或删除一个日志服务器

【命令作用】增加或删除一个日志服务器，包括日志服务器的 IP 地址，服务端口，日志信息的级别等信息

【命令格式】config syslog [add|delete] server <A.B.C.D>{[port] <1-65535>}*1 {[facility] <0-7>}*1

【参数说明】选择 add 表示增加一个日志服务器，选择 delete 表示删除一个日志服务器；A.B.C.D 表示是日志服务器 server 的 IP 地址，port 是日志服务器上接收日志进程的服务端口号，facility 对应于日志信息的级别,就是说这个日志服务器将保存某个级别和某个级别以上的日志信息。

【命令模式】配置模式

【使用指导】可以使用一条命令配置日志服务器信息，也可以使用多条子命令进行配置。关于日志服务器服务程序的配置详见相关手册。

【配置实例】配置了一个 IP 地址为 10.12.3.4 的日志服务器，服务端口为 8808，facility 为 5：

```
Harbour(config)#config syslog add server 10.12.3.4 port 8808 facility 5
Successfully added syslog server 10.12.3.4
```

删除了一个日志服务器，其 IP 地址为 10.1.4.1，服务端口为 6500，facility 为 1：

```
Harbour(config)#config syslog delete server 10.1.4.1 port 6500 facility 1
Successfully deleted syslog server 10.1.4.1
```

10.4 配置日志信息的显示方式

10.4.1 打开或关闭终端显示日志信息的功能

【命令作用】配置日志信息是否输出到用户终端

【命令格式】config syslog monitor-terminal [enable|disable]

【参数说明】选择 enable 表示允许日志信息输出到客户端，选择 disable 表示不允许日志信息输出到客户端

【命令模式】配置模式

【使用指导】该命令是服务命令，将对所有终端起作用。

【配置实例】允许日志信息输出到所有用户终端：

```
Harbour(config)#config syslog monitor-terminal enable

Successfully changed syslog service logto monitor-terminal to
  enable.
```

10.4.2 打开或关闭在本终端显示日志信息的功能

【命令作用】决定是否在本终端输出日志信息

【命令格式】monitor [on|off]

【参数说明】选择 on 表示允许在本终端输出日志信息，选择 disable 表示不允许在本终端输出日志信息。

【命令模式】配置模式

【使用指导】该命令只对本终端起作用。

【配置实例】允许日志信息输出到自己的终端：

```
Harbour(config)#monitor on

Successfully changed your terminal display syslog messages.
```

10.4.3 配置是否显示时间信息

【命令作用】决定是否在本终端输出时间信息

【命令格式】monitor timestamp [none|time|datetime]

【命令模式】配置模式

【使用指导】该命令主要用来决定是否在本终端输出时间信息。

【配置实例】将在本终端输出时间信息：

```
Harbour(config)#monitor timestamp datetime
```

10.4.4 配置在终端可以显示的日志信息的最低级别

【命令作用】决定在本终端输出某一级别和某一级别以上的日志信息

【命令格式】monitor lowest-level <0-7>

【命令模式】配置模式

【使用指导】该命令只对本终端起作用，目前支持的日志信息级别从 0 到 7，依次为 EMERG，ALERT，CRITERR，CRIT，ERR，WARNING，NOTICE，INFO，DEBUG。

【配置实例】将在本终端输出级别 3 和级别 3 以上类型的日志信息：

```
Harbour(config)#monitor lowest-level 3
Successfully changed monitor lowest-lever level 3 [ERR]。
```

10.4.5 配置在终端可以显示的日志信息类型

【命令作用】决定在本终端输出某一类型的日志信息

【命令格式】monitor type [<typename>|all] [on|off]

【命令模式】配置模式

【使用指导】该命令只对本终端起作用，typename 为系统中支持的日志类型，可用 show syslog configuration 来查看日志类型，目前支持的类型有：AUTH，BGP，CLI，SYSLOG，DEVCTRL，ARP，DOT1X，NAS，OSPF，PORT，FDB，RADIUS，RIP，ROUTE，SNMP，STP，SYSTEM，VLAN，WEB，SERVICE，DHCPR 等。all 代表以上支持的所有日志类型。

【配置实例】将在本终端输出所有类型的日志信息：

```
Harbour(config)#monitor type all on
Successfully changed to display all messages.
```

10.5 查看日志管理的配置情况

10.5.1 查看整个日志管理的配置信息

【命令作用】显示日志管理的所有配置信息，包括各种服务的打开和关闭情况等。

【命令格式】show syslog configuration

【命令模式】配置模式

【使用指导】可以列出日志管理的所有配置信息，对使用日志管理命令具有一定指导作用。

【配置实例】

```
Harbour(config)#show syslog configuration
-----------------------------------------------------
Syslog Service is up.
--Service Syslog logto flashfile is up.
--Service Syslog logto server is down.
Have no syslog server.
```


--Service Syslog logto monitor-terminal is up.

--Log messages that not lower than level 4 [WARNING].

--Log these types messages:

--Not log these types messages:

:AUTH:BGP:CLI:SYSLOG:DEVCTRL:ARP:DOT1X:NAS:OSPF:PORT:FDB

:RADIUS:RIP:ROUTE:SNMP:STP:SYSTEM:VLAN:WEB:SERVICE:DHCPR

Record command-line is disabled

10.5.2 查看对本终端的日志显示属性的配置情况

【命令作用】包括所配置的可以在本终端显示的日志类型，日志级别以及时间信息等

【命令格式】show monitor configuration

【命令模式】配置模式

【使用指导】该命令只对本终端起作用。

【配置实例】

Harbour(config)#show monitor configuration

Monitor has been on.

Monitor show messages with none timestamp.

Monitor only display log messages that not lower than level 7 [DEBUG].

Monitor display messages of these types:

Monitor donot display messages of these types:

AUTH:BGP:CLI:SYSLOG:DEVCTRL:ARP:DOT1X:NAS:OSPF:PORT:FDB:RADIUS

:RIP:ROUTE:SNMP:STP:SYSTEM:VLAN:WEB:SERVICE:DHCPR:

10.6 日志模块命令列表

表 10-1 日志模块命令列表

<table>
<tr><th>命令</th><th>描述</th></tr>
<tr><td>config syslog [enable|disable]</td><td>起用或关闭日志服务功能。enable 表示起用，disable 表示关闭。</td></tr>
<tr><td>config syslog monitor-terminal [enable|disable]</td><td>允许或禁止把日志信息输出到终端。enable 表示允许，disable 表示禁止。</td></tr>
<tr><td>config syslog lowest-level <0-7></td><td>配置所要记录的日志信息的最低级别。表示系统将对等于或大于 lowest-level 的日志类型做日志信息。0: 系统不可用，1：实时操作，2：严重，3:错误， 4:告警，5: 提示，6: 一般信息， 7：调试</td></tr>
<tr><td>config syslog type [<name>|all] [enable|disable]</td><td>起用或关闭某一个日志类型或所有日志类型的日志功能。name 为该日志类型名字，all 表示代表所有日志类型。enable 表示起用，disable 表示关闭。</td></tr>
<tr><td>record command-line [enable|disable]</td><td>是否对命令行操作做日志记录。enable 表示允许，disable 表示禁止。</td></tr>
<tr><td>config syslog server [enable|disable]</td><td>允许或禁止把日志信息输出到日志服务器。enable 表示允许，disable 表示禁止。</td></tr>
<tr><td>config syslog [add|delete] server <A.B.C.D> {[port] <1-65535>}*1 {[facility] <0-7>}*1</td><td>配置或删除一个日志服务器。<A.B.C.D>为 IP 地址，port 为端口，facility 为日志信息的级别。</td></tr>
<tr><td>show syslog configuration</td><td>显示日志模块所有配置信息。</td></tr>
<tr><td>monitor [on|off]</td><td>开始显示或结束日志信息输出到本终端。</td></tr>
<tr><td>monitor timestamp [none|time|datetime]</td><td>允许在本终端输出时间信息。</td></tr>
<tr><td>monitor lowest-level <0-7></td><td>设置本终端所要输出的日志信息的级别。该命令执行后，在本终端只显示等于或大于该级别的日志信息。</td></tr>
<tr><td>monitor type [<typename>|all] [on|off]</td><td>设置哪些日志类型的的日志信息可以输出到本终端。</td></tr>
<tr><td>show monitor configuration

record valid-access [enable|disable]</td><td>显示对日志信息输出到本终端的配置信息。
打开或关闭有效用户通过 telnet 登录成功的日志记录功能。</td></tr>
</table>

第11章 网络管理服务 NMS

本章主要包括以下内容：

- NMS 概述
- NMS 功能基本配置
- 在配置表里添加/删除 IP 地址
- 查看 NMS 的配置
- NMS 命令列表

11.1 NMS 概述

NMS(Net Management service)网络管理服务是用来实现访问控制、提高系统的安全性。通常情况下，只要用户拥有登录名和密码就可以登录到交换机，但有时我们出于安全性的考虑，希望用户的 IP 地址是某个特定的或是一个范围，这时就可以打开控制访问服务，将 IP 地址加入到访问配置表。当用户登录时，交换机首先验证该用户 IP 地址的合法性，如果 IP 合法，才会验证用户名和密码的合法性。系统最多允许创建 10 个访问控制配置表。

11.2 NMS 访问控制基本配置

11.2.1 打开或关闭访问控制服务

【命令作用】打开或关闭访问控制

【命令格式】config access-control {[telnet|snmp]}*1 [on|off]

【参数说明】选择 on 表示打开访问控制服务；选择 off 表示关闭访问控制服务

【命令模式】配置模式

【配置实例 1】打开访问控制功能，包括 telnet 和 snmp

```
Harbour(config)#config access-control on
Successfully changed access-control on.
```

【配置实例 2】打开 telnet 访问控制功能

```
Harbour(config)#config access-control telnet on
Successfully changed telnet access-control on
```

11.2.2 创建一个 NMS 访问控制配置

【命令作用】创建一个 NMS 访问控制配置

【命令格式】create nms-access-profile <access_profile_name>

【参数说明】<access_profile_name> 用户创建的访问控制配置的名称，不能超过 20 个字符。

【命令模式】配置模式

【配置实例】创建了一个名称为 admin 的访问控制

```
Harbour(config)#create nms-access-profile admin
Profile admin added success.
```

11.2.3 删除特定的 NMS 访问控制配置

【命令作用】删除特定的 NMS 访问控制配置

【命令格式】delete nms-access-profile <access_profile_name>

【参数说明】<access_profile_name>访问控制配置名称，不能超过 20 个字符。

【命令模式】配置模式

【配置实例】删除名称为 admin 的访问控制配置

```
Harbour(config)#delete nms-access-profile admin
Profile admin delete success.
```

11.2.4 允许或禁止 Telnet 访问控制

【命令作用】允许或禁止 Telnet 访问控制

【命令格式】config nms-access-profile <access_profile_name> telnet [enable|disable]

【参数说明】<access_profile_name>访问控制配置名称，不能超过 20 个字符。

选择 enable 表示打开 telnet 访问控制；选择 disable 表示关闭访问控制。

【命令模式】配置模式

【配置实例】允许 admin 进行 telnet 访问控制

```
Harbour(config)#config nms-access-profile admin telnet enable
Config profile admin's telnet-access enable success.
```

11.2.5 允许或禁止 SNMP 访问控制

【命令作用】允许或禁止 SNMP 访问控制

【命令格式】config nms-access-profile <access_profile_name> snmp [enable|disable]

【参数说明】<access_profile_name>访问控制配置名称，不能超过 20 个字符。

选择 enable 表示打开 telnet 访问控制；选择 disable 表示关闭访问控制。

【命令模式】配置模式

【配置实例】允许 admin 进行 SNMP 访问控制

```
Harbour(config)#config nms-access-profile admin snmp enable
Config profile admin's snmp-access enable success.
```

11.3 在配置表里添加/删除 IP 地址

11.3.1 在指定的配置表里添加 IP 地址

【命令作用】在指定的配置表里添加 IP 地址

【命令格式】config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D/M>
或 config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D> <A.B.C.D>

【参数说明】<A.B.C.D/M> 和<A.B.C.D> <A.B.C.D>分别是两种 IP 地址和子网掩码的表示方式

【命令模式】配置模式

【配置实例】在 admin 配置表里成功地添加 IP 地址 10.5.3.1,子网为 255.255.255.0

```
Harbour(config)#config nms-access-profile admin add ipaddress 10.5.3.1/24
```

或

```
Harbour(config)#config nms-access-profile admin add ipaddress 10.5.3.1
                 255.255.255.0
```

11.3.2 在指定的配置表里删除 IP 地址

【命令作用】在指定的配置表里删除 IP 地址

【命令格式】config nms-access-profile <access_profile_name> delete ipaddress [all |<A.B.C.D/M>]
或 config nms-access-profile <access_profile_name> delete ipaddress <A.B.C.D> <A.B.C.D>

【参数说明】选择 all 表示删除该配置表的所有 IP；<A.B.C.D/M> 和<A.B.C.D> <A.B.C.D>分别是两种 IP 地址和子网掩码的表示方式

【命令模式】配置模式

【配置实例】在 admin 配置表里成功地删除 IP 地址 10.5.3.1,其子网为 255.255.255.0

```
Harbour(config)#config nms-access-profile admin delete ipaddress
                10.5.3.1/24
```

或

```
Harbour(config)#config nms-access-profile admin delete ipaddress
                 10.5.3.1 255.255.255.0
```

11.4 查看访问控制的配置

11.4.1 查看访问控制功能是否打开

【命令作用】查看访问控制功能是否打开

【命令格式】show access-control {[telnet|snmp]}*1

【命令模式】配置模式

【配置实例 1】查看所有的访问控制

```
Harbour(config)#show access-control

Telnet access-control is : on
SNMP  access-control is : on
```

【配置实例 2】只查看 telnet 的访问控制是否打开

```
Harbour(config)#show access-control telnet

Telnet access-control is:on
```

11.4.2 查看特定配置表的配置情况

【命令作用】查看特定配置表的配置情况

【命令格式】show nms-access-profile {<access_profile_name>}*1

【参数说明】<access_profile_name>表示查看指定的访问控制配置表，不加参数表示查看所有配置。

【命令模式】配置模式

【配置实例】查看 admin 的配置情况

```
Harbour(config)#show nms-access-profile admin

==============================================================
Access profile name  : admin
Telnet access status : disable
SNMP   access status : disable
----------------------------------------------------------------
Address List:
----------------------------------------------------------------
No   ID   Network-IP          NetMask
----------------------------------------------------------------
1    0    10.5.5.1            255.255.255.0
2    1    10.5.3.0            255.255.255.0
----------------------------------------------------------------
Total 2 Addresses.
==============================================================
```

11.5 访问控制命令列表

表 11-1 访问控制命令列表

命令	描述
config access-control { [telnet|snmp] }*1 [on|off]	打开或关闭访问控制。选择 on 表示打开；选择 off 表示关闭。
create nms-access-profile <access_profile_name>	创建一个访问控制配置。
delete nms-access-profile <access_profile_name>	删除特定的访问控制配置。
config nms-access-profile <access_profile_name> telnet [enable|disable]	允许或禁止 telnet 访问控制。
config nms-access-profile <access_profile_name> snmp [enable|disable]	允许或禁止 SNMP 访问控制。
config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D/M>	在指定的配置表里添加 IP 地址。
config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D> <A.B.C.D>	在指定的配置表里添加 IP 地址。
config nms-access-profile <access_profile_name> delete ipaddress [all |<A.B.C.D/M>]	在指定的配置表里删除 IP 地址。
config nms-access-profile <access_profile_name> delete ipaddress <A.B.C.D> <A.B.C.D>	在指定的配置表里删除 IP 地址。
show access-control {[telnet|snmp]}*1	查看访问控制功能是否打开。
show nms-access-profile {<access_profile_name>}*1	查看特定配置表的配置情况。

第12章 ACL 配置

12.1 ACL 概述

访问控制列表 ACL（Access Control List）是十分重要的条件列表，可以实现基于 MAC 地址、IP 地址、TCP/UDP 端口等包头字段的接入控制。它在网段之间实现强大的控制访问功能，过滤不需要的数据包和实现安全策略。

µHammer3550-24/µHammer3550-48 的 ACL 配置规则如下：

- ACL的缺省方式是permit any，也就是说当使能ACL功能但是没有配置任何ACL规则的时候，所有的数据包都可以不受ACL的约束正常转发。
- 在没有配置优先级的条件下，执行ACL规则时采用自下向上匹配方式，即后配置的ACL规则先匹配。
- 具有优先级的概念，优先级高的ACL规则先匹配。

12.2 ACL 相关配置

12.2.1 启动/关闭 ACL 服务

【命令格式】service acl [enable|disable]

【使用指导】使能或者关闭 ACL 功能，如果选择 enable 表示使能 ACL 功能，如果选择 disable 表示关闭 ACL 功能

【命令模式】配置模式

12.2.2 添加基于 IP 的 ACL 配置

【命令格式】create acl <name> ip DIP [<A.B.C.D/M>|any] SIP [<A.B.C.D/M>|any] [permit |deny] ports [<portlist>|any]{precedence <0-255>}*1

【使用指导】生成并添加一条针对 IP 数据包的 ACL 策略。可匹配的内容为目的 IP 和源 IP 或任意值，并指定相应的物理端口号；precedence 为可选参数，指定策略的优先级(0-255)，默认为最低 0。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#create  acl  test_ip  ip  DIP  10.1.30.1/16  SIP
  10.1.40.8/16 deny ports any precedence 30
Harbour(config)#show acl all

ACL test_ip ip DIP 10.1.30.1/16 SIP 10.1.40.8/16 deny ports any
  precedence 30
```

12.2.3 添加基于 UDP 的 ACL 配置

【命令格式】create acl <name> udp DIP[<A.B.C.D/M>|any]ip-port [<dst_port>|any] SIP[<A.B.C.D/M>|any] ip-port [<src_port>|any][permit|deny] ports [<portlist>|any] {precedence <0-255>}*1

【使用指导】生成并添加一条针对 UDP 的 ACL 策略。可匹配的内容为目的 IP、源 IP、目的端口号和源端口号或它们任意值，并指定相应的物理端口号，precedence 为可选参数，指定策略的优先级（0-255），默认为最低 0。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#create acl test_udp udp DIP any ip-port 800 SIP any
  ip-port 400 deny ports any precedence 10
Harbour(config)#sh acl all

ACL test_udp udp DIP any ip-port 800 SIP any ip-port 400 deny ports
  any
precedence 10
```

12.2.4 添加基于 TCP 的 ACL 策略

【命令格式】create acl <name> tcp DIP [<A.B.C.D/M>|any] ip-port[<dst_port>|any] SIP [<A.B.C.D/M>|any]ip-port[<src_port>|any][permit|deny]ports [<portlist> |any]{precedence <0-255>}*1

【使用指导】生成并添加一条针对 TCP 的 ACL 策略。可匹配的内容为目的 IP、源 IP、目的端口号和源端口号或它们任意值，并指定相应的物理端口号， precedence 为可选参数，指定策略的优先级（0-255），默认为最低 0。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#create acl test_tcp tcp DIP 11.1.30.1/24 ip-port 800
  SIP 11.1.0.1/24 ip-port 400 deny ports any precedence 7
Harbour(config)#sh acl all

ACL test_tcp tcp DIP 11.1.30.1/24 ip-port 800 SIP 11.1.0.1/24 ip-port
  400 deny
ports any precedence 7
```

12.2.5 添加基于 ICMP 的 ACL 策略

【命令格式】create acl <name> icmp DIP [<A.B.C.D/M>|any]SIP [<A.B.C.D/M>|any] type [<icmp_type>|any] code [<icmp_code>|any] [permit|deny] ports [<portlist>|any] {precedence <0-255>}

【使用指导】生成并添加一条针对 ICMP 数据包的 ACL 策略。可匹配的内容为目的 IP 和源 IP 或任意值，ICMP 类型字段和 ICMP 代码字段，并指定相应的物理端口号， precedence 为可选参数，指定策略的优先级（0-255），默认为最低 0。

【命令模式】配置模式

12.2.6 添加基于 MAC+IP 的 ACL 策略

【命令格式】create acl <name> mac-ip destination [<dst_mac> |any] [<A.B.C.D/M> |any] source [<src_mac> |any] [<A.B.C.D/M>|any] [permit|deny] ports [<portlist>|any] {precedence <0-255>}*1

【使用指导】生成并添加一条针对 MAC+IP 数据包的 ACL 策略。可匹配的内容为目的 IP 和源 IP，目的 MAC 和源 MAC 或任意值，并指定相应的物理端口号， precedence 为可选参数，指定策略的优先级（0-255），默认为最低 0。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#create   ACL   test_macip   mac-ip   destination
  001122334455
11.40.1.1/16 source 001234565566 11.1.30.1/16 deny ports
any precedence 100
Harbour(config)#sh acl all

ACL test_macip mac-ip destination 001122334455 11.40.1.1/16 source
  001234565566
11.1.30.1/16 deny ports any precedence 100
```

12.2.7 删除 ACL 策略

【命令格式】delete acl [<name>|all]

【使用指导】删除相应（name）的 ACL 策略，参数为 all 时删除所有 ACL 策略。

【命令模式】配置模式

12.2.8 查看 ACL 策略

【命令格式】show acl [<name>|all]

【使用指导】显示相应（name）的 ACL 策略，参数为 all 时显示已配置的所有 ACL 策略。

【命令模式】配置模式

12.2.9 设置计数器（counter）

可以为创建的某条 ACL 策略设置一个计数器 counter，用以记录符合这条 ACL 策略的报文数。counter 相关的命令如表 12-1 所示：

表 12-1counter 相关的命令

create counter <name>	创建一个计数器
config acl <name> counter <name>	将创建的计数器与某个已创建的 ACL 策略相关联

	相关联
clear counter [<name>|all]	对某个计数器或所有计数器清零
no acl <name> counter	取消计数器与 ACL 策略的关联
delete counter [<name>|all]	删除某个计数器或所有计数器
show counter [<name>|all]	显示某个计数器或所有计数器

第13章 SNTP 协议

本章包括如下内容：

- SNTP 协议介绍
- SNTP 的相关配置
- 显示 SNTP 配置信息
- 使用举例

13.1 SNTP 概述

13.1.1 SNTP 协议介绍

SNTP（Simple Network Time Protocol）简单网络时间协议，它是用来使网络中的设备能维持相同的时间的一种通信协议，通过在网络设备中运行 SNTP 协议，有利于网络中设备的管理和维护。SNTP 协议采用客户端、服务器的方式。

13.1.2 SNTP 的三种工作模式

SNTP 协议在维护网络设备的时间时有三种不同的工作模式：

Unicast：客户端通过向指定的服务器发出包含本地时间请求的报文，服务器在响应报文中包含服务器接收到客户端请求报文的时间和服务器发出响应报文的时间。客户端在收到服务器的响应报文后，通过报文中包含的各种时间值可以计算出报文的循环周期以及本地设备的时间值和服务器的偏差。

Multicast：服务器端周期性的广播自己的时间值，客户端在接收到广播报文后，把自己的时间值改为和服务器广播报文中的时间值一致。

Anycast：当客户端不知道时间服务器的地址时采用此种方式，即客户端向指定的网络发出多播或广播请求报文，网络中的服务器在收到广播请求报文后，都以单播的方式响应客户端，但客户端只接收最先收到的响应报文，并记录下此服务器的地址。以后客户端和此服务器便工作在 unicast 模式下了。

13.2 配置 SNTP

在交换机上配置 SNTP 包含以下内容：

- 配置 SNTP 客户端或 SNTP 服务器的工作模式
- 使能（使 SNTP 客户端有效）或关闭 SNTP 的客户端
- 使能（使 SNTP 服务器有效）或关闭 SNTP 的服务器
- 配置 SNTP 客户端的各种参数

13.2.1 使能或关闭 SNTP 客户端

在一台 Hammer 交换机中 SNTP 客户端的缺省状态是关闭的。

【命令格式】config sntp-client [enable | disable]

【参数说明】如果键入 enable，表示使能运行 SNTP 客户端，如果键入 disable，则表示关闭运行 SNTP 的客户端。

【使用指导】在启动 SNTP 客户端以前必须先配置 SNTP 的工作模式。

【命令模式】配置模式

13.2.2 使能或关闭 SNTP 服务器

在一台 Hammer 交换机中 SNTP 服务器的缺省状态是关闭的。

【命令格式】config sntp-server [enable | disable]

【参数说明】如果键入 enable，表示开始运行 SNTP 服务器，如果键入 disable，则表示取消运行 SNTP 服务器。

【使用指导】在启动 SNTP 服务器以前必须先配置 SNTP 的工作模式。

【命令模式】配置模式

13.2.3 配置 SNTP 的工作模式

SNTP 的工作模式表明了网络中的时间协议以哪种方式来工作，SNTP 协议支持三种工作模式：unicast，multicast，anycast，缺省值为 unicast 模式。在运行 SNTP 之前一定要配置好 SNTP 的工作模式，一旦 SNTP 启动后，就不能再对它的工作模式进行修改了。

【命令格式】cofig [sntp-client | sntp-server] mode <1-3>

【参数说明】如果键入 sntp-client 表示配置客户端的工作模式，如果键入 sntp-server 表示配置服务器端的工作模式。参数<1-3>分别代表 unicast，multicast，anycast。

【命令模式】配置模式

【配置实例】配置 sntp 的客户端的工作模式是 unicast

```
Harbour(config)#config sntp-client mode 1
```

13.2.4 配置客户端的 SNTP 服务器的 IP 地址

当 SNTP 客户端工作在 unicast 模式下时，在启动 SNTP 之前一定要先配置 SNTP 服务器的 IP 地址，以便客户端能和指定的服务器之间进行通信。

【命令格式】config sntp-client server ipaddr <A.B.C.D >

【参数说明】<A.B.C.D >为 SNTP 服务器的 IP 地址。

【命令模式】配置模式

【配置实例】配置客户端的服务器的 IP 地址为 10.5.4.66

```
Harbour(config)#config sntp-client server ipaddr 10.5.4.66
```

13.2.5 配置客户端的刷新周期

客户端的刷新周期是指客户端每隔多长时间向服务器端发起一次时间请求报文。当客户端工作在 anycast 和 unicast 模式下时，需要配置客户端的时间刷新周期。

【命令格式】config sntp-client update-interval <64-1024>

【参数说明】参数<64-1024>表示客户端刷新周期时间值，单位是秒，缺省值为 64（s）

【命令模式】配置模式

【配置实例】将客户端的刷新周期设置为 100 秒

```
Harbour(config)#config sntp-client update-interval 100
```

13.2.6 配置服务器端的广播周期

在 SNTP 的服务器工作在 multicast 模式下时，服务器以一定的周期向指定的网络中广播自己的时间值。

【命令格式】config sntp-server broadcast-interval <64-1024>

【参数说明】参数<64-1024>表示服务器端的广播周期，缺省值为 64（s）。

【命令模式】配置模式

【配置实例】配置时间服务器的广播周期为 66（s）

```
Harbour(config)#config sntp-server broadcast-interval 66
```

13.2.7 恢复 SNTP 客户端的工作模式为 unicast 模式

【命令格式】no sntp-client mode

【命令模式】接口模式

【配置实例】在 sntp 客户端关闭的状态下，想要恢复 sntp 客户端的工作模式为 unicast 模式

```
Harbour(config-if)#no sntp-client mode
```

13.2.8 恢复 SNTP 服务器的工作模式为 unicast 模式

【命令格式】no sntp-server mode

【命令模式】接口模式

【配置实例】在 sntp 服务器关闭的状态下，想要恢复 sntp 服务器的工作模式为 unicast 模式

```
Harbour(config-if)#no sntp-server mode
```

13.2.9 恢复 SNTP 客户端的缺省刷新周期

【命令格式】no sntp-client update-interval

【命令模式】接口模式

【配置实例】想要恢复 sntp 客户端的缺省刷新周期时间值（64s）：

```
Harbour(config-if)#no sntp-client update-interval
```

13.2.10 恢复 SNTP 服务器的缺省广播周期

【命令格式】no sntp-server broadcast-interval

【命令模式】接口模式

【配置实例】想要恢复 sntp 服务器端的缺省广播周期时间值（64s）：

```
Harbour(config-if)#no sntp-server broadcast-interval
```

13.3 显示 SNTP 的状态信息

13.3.1 显示客户端的状态

【命令格式】show sntp-client

【使用指导】show 命令所显示的 SNTP 客户端的信息包括以下内容：

- 客户端的工作模式
- 时间服务器的IP地址
- 时间请求的发送间隔
- SNTP是否启动

【配置实例】显示 SNTP 客户端的配置信息：

```
Harbour(config)#show sntp-client

------------sntp client's current state--------------
sntp-client are running.
sntp-client's mode is unicast.
sntp-server's IPAddress is 10.5.4.66.
sntp-client's update-interval is 64 seconds.
```

13.3.2 显示服务器端的状态

【命令格式】show sntp-server

【使用指导】show 命令所显示的 SNTP 服务器端的信息包括以下内容：

- 服务器端的工作模式
- 服务器的时间广播周期
- SNTP是否启动

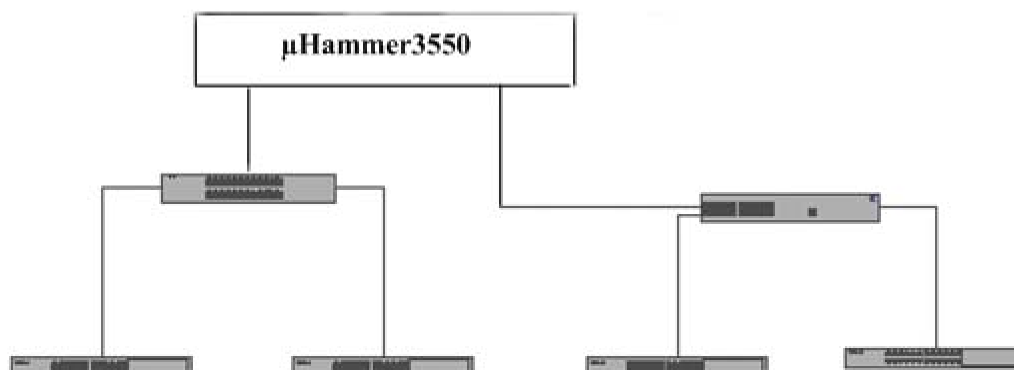
【配置实例】显示 SNTP 服务器端的配置信息：

```
Harbour(config)#show sntp-server

------------sntp server's current state--------------
sntp-server is running.
sntp-server's mode is unicast.
```

13.4 SNTP 协议配置举例

按下图的例子对一个二层网络实现 SNTP 的配置：



1、在µHammer3550 交换机上创建一个时间服务器，使其工作在 anycast 模式下（当然也可以采用 unicast 或者 multicast 模式）：

Harbour(config)#config sntp-server mode 3

Harbour(config)#config sntp-server enable

2、然后在需要同步时间的交换机上键入如下命令：

Harbour(config)#config sntp-client mode 3

Harbour(config)#config sntp-client enable

3、为了适应不同的精确性要求，用户也可以对交换机的时间更新频率进行修改。例如把时间校正周期调整到 100（s）：

Harbour(config)#config sntp-client update-interval 100

第14章 虚拟堆叠

14.1 堆叠概述

堆叠技术是目前在以太网交换机上扩展端口使用较多的一种技术，是一种非标准技术。各厂商不支持混合堆叠，堆叠模式为各厂商自行制定。它将一组相互连接在一起的交换机当作一个整体来看待，实现系统的简易本地化集中管理，简化和方便整体操作。目前流行的堆叠有两种主要形式：菊花链模式和星型模式：

- 菊花链模式是一种基于堆叠的技术，对交换机的硬件没有特殊的要求，通过相对高速的端口串连和软件支持，最终构建一个多交换机的环状结构。
- 星型堆叠是一种高级堆叠技术，对交换机而言，需要提供一独立的高速交换中心，所有主机通过高速堆叠端口连接到同一的堆叠中心。

µHammer3550-24/µHammer3550-48 是港湾公司最近开发的具有堆叠功能的新一代交换机，它具备目前流行的堆叠功能，并且支持菊花链和星型两种模式。使用堆叠功能可以为用户带来以下好处：

- 管理交换机不受空间的限制，它们可以都在本地也可以在远端，只要是在堆叠管理VLAN二层网络能够到达的地方，就可以管理到
- 节省资源，简化重复性的耗时工作
- 节省IP

由于实现的是三层堆叠，存在虚 IP 的概念。默认情况下堆叠服务是打开的，并且系统为每个交换机分配了一虚拟的 IP，系统默认的虚拟 IP 为 172.30.0.1/24 网段，如果该网段同用户的所有网段不冲突的话，用户不必关心该网段；如果同用户的所用网段冲突，用户可以通过手工的方式指定不冲突网段。目前的版本有些应用是基于三层的，所以用户在操作时应先设置好路由，以确保交换机能同网管站连通。

14.2 虚拟堆叠配置

14.2.1 启动或者关闭堆叠功能

【命令格式】`[start|stop] cluster`

【参数说明】启动或禁止堆叠功能，默认为启动状态，可以手工关闭

【命令模式】配置模式

14.2.2 配置 commander switch

【命令格式】`config cluster commander`

【参数说明】配置一台交换机作为堆叠系统的 `commander`，一个堆叠系统中只允许设置一台

Command switch

【命令模式】配置模式

14.2.3 查看堆叠成员信息

【命令格式】show cluster

【参数说明】查看堆叠系统中的交换机信息，其中 ID 为 0 的为 Command switch 其余为 Member switch

【命令模式】配置模式

【配置实例】

```
Harbour(config)#show cluster

The system is commander,stack cluster information...........
----------------------------------------------------------------
  ------------
|ID      |duty       |deviceType           |stackPort |macAddress
  |
----------------------------------------------------------------
  ------------
| 0        |  commander|  uHammer3550-24         |  0            |
  00-05-3b-00-04-91     |
----------------------------------------------------------------
  ------------
| 1        |  member     |  uHammer3550-24         |  6            |
  00-05-3b-00-38-99     |
----------------------------------------------------------------
  ------------
| 2        |  member     |  uHammer3550-24         |  6            |
  00-05-3b-58-00-52     |
----------------------------------------------------------------
  ------------
| 3        |  member     |  uHammer3550-24         |  11           |
  00-05-3b-58-00-32     |
----------------------------------------------------------------
  ------------
| 4        |  member     |  uHammer3550-24         |  6            |
  00-05-3b-00-04-90     |
----------------------------------------------------------------
  -----------
```

14.2.4 配置某一台交换机

【命令格式】config cluster member <1-7>

【参数说明】对一个堆叠系统中的一台交换机进行配置

【命令模式】配置模式

14.2.5 选择一组交换机升级

【命令格式】cluster download ftp [hammeros|config-file] <A.B.C.D> <username> <password> <filename> [<clusterlist>|all]

【参数说明】对一个堆叠系统中的一组交换机进行升级

【命令模式】配置模式

14.2.6 选择一组交换机保存配置

【命令格式】cluster save [<clusterlist>|all]

【参数说明】对一个堆叠系统中的一组交换机进行保存配置

【命令模式】配置模式

14.2.7 选择一组交换机擦除配置

【命令格式】cluster erase [<clusterlist>|all]

【参数说明】对一个堆叠系统中的一组交换机的配置进行擦除

【命令模式】配置模式

14.2.8 选择一组交换机重新起动

【命令格式】cluster reboot [<clusterlist>|all]

【参数说明】对一个堆叠系统中的一台交换机进行重新启动

【命令模式】配置模式

14.2.9 配置堆叠系统的 trap receiver

【命令格式】config cluster trap version [v1|v2c] {community <string>}*1

【参数说明】对一个堆叠系统中的所有交换机配置统一的 trap receiver

【命令模式】配置模式

14.2.10 取消堆叠系统的 trap receiver

【命令格式】config cluster trap version [v1|v2c] {community <string>}*1

【参数说明】取消堆叠系统中 trap receiver，使其不再发送堆叠的 trap。

【命令模式】配置模式

14.2.11 查看堆叠系统的 trap 配置

【命令格式】show cluster snmp trap

【参数说明】查看堆叠系统中 trap 配置

【命令模式】配置模式

附录 命令索引

下面的普通用户命令列表和管理员用户列表均以µHammer3550-48 交换机为例，µHammer3550-24 交换机的命令与之相同，只是在标记端口范围<1-50>的地方改成<1-26>即可。

普通用户命令一览表：

<table>
<tr><th>命令名称</th><th>命令功能描述</th></tr>
<tr><td>clear</td><td>清除屏幕</td></tr>
<tr><td>enable</td><td>进入配置模式，可以对交换机进行配置和写操作</td></tr>
<tr><td>exit</td><td>结束当前模式，返回前一模式</td></tr>
<tr><td>help</td><td>显示系统的帮助信息</td></tr>
<tr><td>list</td><td>列出当前模式下的所有命令</td></tr>
<tr><td>logout</td><td>断开与交换机的连接，并退出系统</td></tr>
<tr><td>ping {[-t]}*1 {[-count] <1-65535>}*1 {[-size] <0-6400>}*1 {[-waittime] <1-255>}*1 {[-ttl] <1-255>}*1 {[-pattern] <user_pattern>}*1 <A.B.C.D></td><td>用于检测网络连接是否正常。</td></tr>
<tr><td>quit</td><td>断开与交换机的连接并退出系统</td></tr>
<tr><td>show ACL [<name>|all]</td><td>查看 ACL 策略</td></tr>
<tr><td>show arp {[<A.B.C.D>|permanent]}*1</td><td>查看 arp 地址表项</td></tr>
<tr><td>show fdb {[mac] <macaddr>}*1 {[vlan] <name>}*1</td><td>显示 mac 地址为<macaddr>，vlan 名为<vlan>的 FDB 信息</td></tr>
<tr><td>show fdb agetime</td><td>显示地址表老化时间</td></tr>
<tr><td>show fdb permanent {[mac] <macaddr>}*1 {[vlan] <name>}*1</td><td>显示永久的 FDB 信息</td></tr>
<tr><td>show history</td><td>显示历史命令</td></tr>
<tr><td>show idle-timeout</td><td>显示经过多长的空闲等待时间系统自动进入登录前的状态</td></tr>
<tr><td>show interface {<IFNAME>}*1</td><td>显示接口状态和配置信息</td></tr>
<tr><td>show ip route</td><td>显示 RIB 路由表所有路由信息</td></tr>
<tr><td>show ip route <A.B.C.D/M></td><td>显示 RIB 表中目的 IP 地址和子网掩码长度与<A.B.C.D/M>匹配的路由信息</td></tr>
<tr><td>show ip route <A.B.C.D></td><td>显示RIB表中目的IP地址与<A.B.C.D>匹配的路由信息</td></tr>
<tr><td>show ip route [connected|static]</td><td>显示 RIB 表中指定协议的路由信息</td></tr>
<tr><td>show ip route summary</td><td>查看路由表的详细信息</td></tr>
<tr><td>show mirroring</td><td>查看系统镜像信息</td></tr>
</table>

show port [<portlist>|all] {[configuration|stats]}*1	显示系统指定端口的配置信息或状态
show services	显示系统服务的状态，包括 telnet，snmp， 和 web manage 三个服务
show sharing	显示系统 sharing 信息
show stpd default	显示 STP 域缺省信息
show stpd default port [<portlist> | all]	显示指定端口的 stp 信息
show syscontact	显示管理本主机的用户，以及如何联系该用户
show syslocation	显示主机所在的物理位置
show time	显示系统日期
show version	显示 HammerOS 系统版本信息
show vlan {<name>}*1	显示系统 VLAN 信息
telnet <A.B.C.D>	登录其他主机或者交换机
terminal length <0-512>	设置终端屏幕上所显示的行数
who	显示连接在交换机上的所有用户
who am I	仅仅显示用户自己的连接信息

管理员用户命令一览表：

命令	功能描述
clear	清除屏幕
clear counter [<name>|all]	清空指定名称（name）或所有（all）ACL 计数器的统计信息
clear igmp snooping vlan <name>	清除 VLAN 内的组播
clear ip route static	清除静态路由
clear stats port [<portlist>|all]	清除端口统计信息，选择 portlist 对指定端口进行操作，选择 all 对所有端口进行操作
config ACL <name> priority <0-7>	配置 ACL 策略的数据流的优先级的重新映射
config WRR-queue bandwidth <low,normal,medium,high>	配置队列加权轮循的权重
config access-control {[telnet|web|snmp]}*1 [on|off]	激活或禁止对 telnet、web 和 snmp 的访问控制功能。
config acl <name> counter <name>	设置 ACL 计数器
config igmp snooping host_timeout <10-2147483647>	设置主机超时时间间隔
config igmp snooping router_timeout <10-2147483647>	设置路由器超时时间间隔

config loopDetect [enable|disable]	设置端口的下行环路检测。enable 表示允许，disable 表示禁止。
config mirroring [add|delete] port [<portlist>|all] [egress|ingress]	增加或删除镜像端口的发送或接收包，选择 add 为增加镜像端口，选择 delete 为删除端口，选择 egress 为对发送包进行镜像，选择 ingress 为对接收包进行镜像
config mirroring disable	取消端口镜像
config mirroring to <1-50>	配置镜像目标端口
config fdb agingtime [0|<10-1000000>	修改 fdb 表老化时间
config nms-access-profile <access_profile_name> snmp [enable|disable]	禁止或允许 NMS 访问控制组中的用户使用交换机的 snmp 服务，enable 表示允许，disable 表示禁止
config nms-access-profile <access_profile_name> web [enable|disable]	禁止或允许 NMS 访问控制组中的用户使用交换机的 web 服务
config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D> {netmask [<0-32>|<A.B.C.D>]}*1	向 NMS 访问控制组中加入一个用户 ip 地址
config nms-access-profile <access_profile_name> delete ipaddress <A.B.C.D> {netmask [<0-32>|<A.B.C.D>]}*1	删除 NMS 访问控制组中的用户 ip 地址
config nms-access-profile <access_profile_name> telnet [enable|disable]	禁止或允许 NMS 访问控制组中的用户使用交换机的 telnet 服务，enable 表示允许，disable 表示禁止
config port [<portlist>|all] [enable|disable]	修改端口状态（开/关），enable 为打开端口，disable 为关闭端口
config port [<portlist>|all] auto [on|off]	修改端口自适应状态（开/关），on 为打开端口自适应功能，off 为关闭端口自适应功能
config port [<portlist>|all] duplex [full|half]	修改端口工作方式（全双工/半双工），full 为全双工方式，half 为半双工方式
config port [<portlist>|all] flowcontrol [on|off]	修改端口流控状态（开/关），on 为打开端口流控功能，off 为关闭端口流控功能
config port [<portlist>|all] speed [10|100|1000]	修改端口速度，10 为 10Mbps，100 为 100Mbps，1000 为 1000Mbps
config port [<portlist>|all] learn [on|off]	使能或者禁止端口的地址学习功能
config port [<portlist>|all] mode [master|slave]	千兆电口工作在强制千兆模式下，需要一端设置成主模式，另一端设置从模式。

<table>
<tr><td>config port [<portlist>|all] remap-priority <0-7></td><td>配置相应端口对 802.1p 优先级的重新映射</td></tr>
<tr><td>config port [<portlist>|all] remap-priority [on|off]</td><td>使能/禁止端口对 802.1p 优先级的重新映射功能</td></tr>
<tr><td>config priority <0-7> qosqueue [Low|Normal|Medium|High]</td><td>配置 802.1p 优先级到 CoS 队列的映射关系</td></tr>
<tr><td>config sharing <1-50> select-mode <rtag></td><td>配置 Load sharing 成员端口的转发策略</td></tr>
<tr><td>config snmp community [readonly|readwrite] <string></td><td>设置 community 的 readonly/readwirte 字符串信息</td></tr>
<tr><td>config snmp trapreceiver add <A.B.C.D> version [v1|v2c] {community <string>}*1</td><td>添加一个 trap 接收服务器 Ip 地址</td></tr>
<tr><td>config snmp trapreceiver delete <A.B.C.D></td><td>删除一个 trap 接收服务器 Ip 地址</td></tr>
<tr><td>config stpd default [enable|disable]</td><td>打开或关闭 stpd 功能</td></tr>
<tr><td>config stpd default port [<portlist> | all] cost <1-65535></td><td>修改端口 STP 路径开销值</td></tr>
<tr><td>config stpd default port [<portlist> | all] priority <0-255></td><td>修改端口 STP 优先级</td></tr>
<tr><td>config stpd default port [<portlist>|all] [enable|disable]</td><td>修改端口 STP 状态（参加 STP 计算/不参加 STP 计算）</td></tr>
<tr><td>config stpd default [enable | disable]</td><td>修改 STP 状态（打开/关闭）</td></tr>
<tr><td>config stpd default forwarddelay <4-30></td><td>修改 STP 延迟时间</td></tr>
<tr><td>config stpd default hellotime <1-10></td><td>修改 STP 响应时间</td></tr>
<tr><td>config stpd default maxage <6-40></td><td>修改 STP 最长计算时间</td></tr>
<tr><td>config stpd default priority <0-65535></td><td>修改 STP 优先级</td></tr>
<tr><td>config syscontact <.contact></td><td>描述主机管理员的信息，包括用户名、联系方式等（根据需要来设定）</td></tr>
<tr><td>config syslocation <.location></td><td>描述主机的位置</td></tr>
<tr><td>config time <1970-2100> <1-12> <1-31> <HH:MM:SS></td><td>修改日期时间，依次为年、月、日、时、分、秒</td></tr>
<tr><td>config vlan <name> [add|delete] port <portlist> [tagged|untagged]</td><td>配置名为<name>的 VLAN 的端口为 tagged 或 untagged</td></tr>
<tr><td>config vlan <name> ipaddress <A.B.C.D/M></td><td>配置名为<name>的 VLAN 的 IP 地址和网络掩码长度</td></tr>
</table>

config vlan <name> ipaddress <A.B.C.D> <A.B.C.D>	配置名为<name>的 VLAN 的 IP 地址和网络掩码
config vlan <name> priority <0-7>	通过改变 VLAN 的优先级属性来实现属于某一个 VLAN 的数据流的优先级的重新映射
config vlan <name> tag <1-4094>	配置名为<name>的 VLAN 的标签（即 VLAN ID）
create ACL <name> ip DIP [<A.B.C.D/M>|any] SIP [<A.B.C.D/M>|any] [permit|deny] ports [<portlist>|any] {precedence <0-255>}	创建基于 IP 的 ACL 策略
create ACL <name> udp DIP [<A.B.C.D/M>|any] ip-port [<dst_port>|any] SIP [<A.B.C.D/M>|any] ip-port [<src_port>|any] [permit|deny] ports [<portlist>|any] {precedence <0-255>}	创建基于 UDP 的 ACL 策略
create ACL <name> tcp DIP [<A.B.C.D/M>|any]ip-port [<dst_port>|any] SIP [<A.B.C.D/M>|any]ip-port [<src_port>|any] [permit|deny] ports [<portlist>|any]{precedence <0-255>}*1	创建基于 TCP 的 ACL 策略
create ACL <name> mac-ip destination [<dst_mac> |any] [<A.B.C.D/M> |any] source [<src_mac> |any] [<A.B.C.D/M>|any] [permit|deny] ports [<portlist>|any] {precedence <0-255>}*1	创建基于 MAC+IP 的 ACL 策略
create ACL <name> icmp DIP [<A.B.C.D/M>|any] SIP [<A.B.C.D/M>|any] type [<icmp_type>|any] code [<icmp_code>|any] [permit|deny] ports [<portlist>|any] {precedence <0-255>}*1	创建基于 ICMP 的 ACL 策略
create counter <name>	创建一个计数器
create fdbentry <mac_address> vlan <name> port <portno> {priority <0-7>}*1	创建 FDB 地址表项
create sharing <1-50> grouping <portlist>	创建特定 Load Sharing，这一 Load Sharing 由端口<portlist>组成
create vlan <name>	创建一个名为<name>的 VLAN
delete ACL [<name>|all]	删除一个或所有 ACL 策略
delete counter [<name>|all]	删除一个或所有 ACL 计数器

delete fdbentry {mac <mac_address> vlan <name>}*1	删除转发表中指定的 MAC 地址的入口
delete nms-access-profile <access_profile_name>	删除一个 NMS 访问控制组
delete sharing <1-50>	删除指定的 Load Sharing
delete vlan [<name>|all]	删除名为<name>的 VLAN 或所有的 VLAN
download ftp [hammeros|config-file] <A.B.C.D> <username> <password> <filename>	利用 FTP 下载 HammerOS 文件或 config-file 到 FLASH 中
download xmodem [hammeros|config-file] {baudrate [9600|115200]}*1	利用 xmodem 协议下载 HammerOS 文件或 config-file 到 FLASH 中并可以选择下载带宽为 9600 或 115200
enable-password	修改进入配置模式的密码，必须大于或者等于 6 个字符
erase {startup-config}*1	删除交换机启动配置
exit	关闭当前模式，返回到上一个模式
help	显示系统帮助信息
hostname <hostname>	设置系统的网络名称，例如，在本手册中，网络名称为 HammerOS
idle-timeout <0-35791>	设置经过多长的空闲等待系统自动进入登录前的状态
interface <IFNAME>	进入要配置的 vlan 接口名称
ip route <A.B.C.D/M> [<A.B.C.D>] {<1-255>}*1	建立一条静态路由,目的 IP 地址和子网掩码长度为<A.B.C.D/M>， 下一跳 IP 地址为<A.B.C.D>，distance 值为<1-255>
ip route <A.B.C.D> <A.B.C.D> [<A.B.C.D>] {<1-255>}*1	建立一条静态路由,目的 IP 地址为第一个<A.B.C.D>,子网掩码为第二个<A.B.C.D>,下一跳地址为第三个<A.B.C.D>，distance 值为<1-255>
kill session <1-24>	强制断开特定 telnet 连接
list	列出当前模式下的所有命令
List<pattern>	根据关键字查找命令行
login-password	设置登录密码
logout	断开与交换机的连接并退出系统
monitor [on|off]	打开或关闭在本终端显示日志信息的功能
monitor lowest-level <0-7>	配置在终端可以显示的日志信息的最低级别
monitor timestamp [none|time|datetime]	配置是否显示时间信息
monitor type [<typename>|all] [on|off]	配置在终端可以显示的日志信息的类型
no acl <name> priority	取消已经配置的 ACL 优先级配置信息

<table>
<tr><td>no ip route <A.B.C.D/M> <A.B.C.D> {<1-255>}*1</td><td>删除目的网段 IP 地址和子网掩码长度为<A.B.C.D/M>、下一跳地址为<A.B.C.D>、distance 值(如果有)为<1-255>的静态路由</td></tr>
<tr><td>no ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> {<1-255>}*1</td><td>删除目的网段 IP 地址为第一个<A.B.C.D>、子网掩码为第二个<A.B.C.D>、下一跳地址为第三个<A.B.C.D>、 distance 值(如果有)为<1-255>的静态路由</td></tr>
<tr><td>no vlan-priority <name></td><td>取消已经配置的 vlan 优先级配置信息</td></tr>
<tr><td>no vlan <name> ip</td><td>删除指定 vlan 的 ip 地址</td></tr>
<tr><td>ping {[-t]}*1 {[-count] <1-65535>}*1 {[-size] <1-6400>}*1 {[-waittime] <1-255>}*1 {[-ttl] <1-255>}*1 {[-pattern] <user_pattern>}*1 <A.B.C.D></td><td>用于检测网络连接是否正常</td></tr>
<tr><td>quit</td><td>断开与交换机的连接并退出系统</td></tr>
<tr><td>reboot</td><td>重新启动交换机</td></tr>
<tr><td>record command-line [enable|disable]</td><td>打开命令行操作日志记录功能</td></tr>
<tr><td>save configuration</td><td>保存系统配置信息</td></tr>
<tr><td>service acl [enable|disable]</td><td>启用或者禁止 acl 功能</td></tr>
<tr><td>service igmp snooping [enable|disable]</td><td>启用/禁止 IGMP Snooping 功能</td></tr>
<tr><td>service qos [enable|disable]</td><td>启用或者禁止 QoS 功能</td></tr>
<tr><td>service snmp [enable|disable]</td><td>启用或者禁止 snmp 功能</td></tr>
<tr><td>service snmp rmon [enable|disable]</td><td>启用或者禁止 rmon 功能</td></tr>
<tr><td>service snmp trap [enable|disable]</td><td>启用或者禁止 snmp trap 功能</td></tr>
<tr><td>service telnet [enable|disable]</td><td>配置 telnet 服务，打开或关闭服务，enable 为打开 telnet 服务，disable 为关闭 telnet 服务</td></tr>
<tr><td>show ACL [<name>|all]</td><td>查看一个或所有 ACL 策略</td></tr>
<tr><td>show WRR-queue</td><td>显示 4 个优先级队列与权重的对应关系</td></tr>
<tr><td>show arp {[<A.B.C.D>|permanent]}*1</td><td>查看 arp 地址表项信息</td></tr>
<tr><td>show acl counter</td><td>查看 ACL 计数信息</td></tr>
<tr><td>show counter [<name>|all]</td><td>查看一个或所有的计数器统计信息</td></tr>
<tr><td>show dot1p-QosQueue-mapping</td><td>显示 802.1p 优先级到 CoS 队列的映射关系</td></tr>
<tr><td>show arp [{<A.B.C.D>}*1 |{permanent}*1]</td><td>显示 IP 地址为<A.B.C.D>的 Arp 表项</td></tr>
<tr><td>show fdb {[mac] <macaddr>}*1 {[vlan] <name>}*1</td><td>显示 mac 地址为<macaddr>，vlan 名为<vlan>的 mac 地址入口信息</td></tr>
<tr><td>show fdb agingtime</td><td>显示 fdb 表的老化时间</td></tr>
</table>

show fdb permanent {[mac] <macaddr>}*1 {[vlan] <name>}*1	显示指定的静态 mac 地址信息
Show fdb summary	显示 FDB 统计信息，包括静态和动态 FDB 信息
Show filter	显示系统 IRULE 和 IMASK 表的信息
show history	显示最近用户输入的 20 个历史命令
show idle-timeout	显示经过多长的空闲等待系统自动进入登录前的状态
show igmp snooping timer	显示 IGMP Snooping 定时信息
show igmp snooping vlan <name>	显示 VLAN 中的 IGMP Snooping
show interface {<IFNAME>}*1	显示接口名称
show ip fib	显示系统当前有效地 IP 转发表
show ip route	显示 RIB 表中所有路由信息
show ip route <A.B.C.D/M>	显示 RIB 表中目的 IP 地址和子网掩码长度与<A.B.C.D/M>匹配的路由信息
show ip route <A.B.C.D>	显示在此 RIB 表中的制定目的 IP 地址（不含子网掩码）的路由信息
show ip route [connected|static]	显示 RIB 表中指定路由协议的路由信息：直连的，通过 rip 协议学到的和静态的
show ip route summary	显示 RIP 路由表概要信息
Show macgroup-info	显示 MAC groupr 的信息
show mirroring	显示镜像配置信息
show monitor{configuration}*1	显示 monitor 的状态是打开还是关闭
show nms-access-profile {<access_profile_name>}*1	显示 NMS 访问控制组的内容
show port [<portlist>|all] {[configuration|stats]}*1	显示系统指定端口的配置信息
show qos [port|mac|vlan|acl|all]	显示不同类型的 QoS 优先级配置信息
show running-config	显示系统的运行配置
show services	显示系统服务的状态，包括 telnet，snmp， 和 web manage 三个服务
show sharing	显示系统 sharing 信息
show snmp community-string	显示 community-string 的 get/set 字符串信息
Show snmp trapagent-address	显示 SNMP 的 trapagent-address 信息
show snmp trapreceiver	查看 snmp trapreceiver 的信息
show startup-config	显示启动配置
show stpd default	显示 STP 域端口信息
show stpd default port [<portlist>| all]	显示指定/全部端口的生成树协议信息
show syscontact	显示描述主机管理员的信息

show syslocation	显示描述主机的位置的信息
show syslog {configuration}*1	显示系统日志信息
show time	显示系统时间信息
show version	显示系统版本信息
show vlan {<name>}*1	显示 VLAN 的信息
telnet <A.B.C.D>	远程登录 IP 地址为<A.B.C.D>的主机或交换机
terminal length <0-512>	设置终端屏幕所显示的行数
upload ftp [hammeros|config-file] <A.B.C.D> <username> <password> <filename>	利用 FTP 上传 HammerOS 文件或 config-file 到文件服务器中
upload xmodem [hammeros|config-file] {baudrate [9600|115200]}*1	利用 xmodem 协议上传 HammerOS 文件或 config-file 到文件服务器中并可以选择下载带宽为 9600 或 115200
user add <username> login-password <login_password>	添加登录密码为<login_password>的用户<username>到系统中
user delete <username>	从系统中删除用户<username>
user enable-password <username>	设置用户<username>的配置密码
user list	显示所有系统用户
user login-password <username>	设置系统用户<username>的登录密码
user role <username> ADMIN enable-password <enable_password>	把用户<username>转变为系统管理员，且密码为<enable_password>
user role <username> NORMAL	把用户<username>转变为普通用户
who	显示连接在交换机上的所有用户
who am i	仅仅显示用户自己的连接信息